# VistA Blood Establishment Computer Software (VBECS) Version 1.4.0.0

## Technical Manual-Security Guide

## May 2009

Department of Veterans Affairs
Office of Enterprise Development

This page intentionally left blank.

# Revision History

| Date | Revision | Description | Author |
|---|---|---|---|
| 6-19-08 | 1.0 | Updates made to VBECS 1.3.0.0 Technical Manual-Security Guide for VBECS 1.4.0.0:<br>Updated the Windows Updates section due to changes caused by Windows Software Update Services implementation. | BBM team |
| 9-12-08 | 2.0 | Updates made to VBECS 1.4.0.0 Technical Manual-Security Guide, Version 1.0 for Version 2.0:<br>Hardware and System Configuration: Added a section called Server and Shared Array Discs.<br>Implementation and Maintenance: Added a section called HP System Utilities and added a table to the Periodic Maintenance Checks section to better explain the schedule of server updates. | BBM team |
| 1-20-09 | 3.0 | Updates made to VBECS 1.4.0.0 Technical Manual-Security Guide, Version 2.0 for Version 3.0:<br>Title Page: Changed "Veterans Health Information Technology" to "Office of Enterprise Development"<br>How This Technical Manual-Security Guide is Organized: Added Screen Shots section.<br>Appendices: Updated second paragraph to better explain table of contents navigation function.<br>Global: Added specific row where information is found when referenced in an appendix.<br>Global: Added a  (camera) icon to each instance where a screen shot is required.<br>Expanded "OU" acronym to "Organizational Unit" at its first occurrence in document.<br>Changed section name from "Hardware Specifications and Settings" to "Remote Desktop Configuration"<br>Changed section name from "Hardware and System Configuration" to "Server Hardware and System Configuration"<br>Changed name of section and Table 1 from "Terminal Server and Database Server Configuration" to "Server Configuration"<br>Changed name of section and Table 2 from "Additional Required Hardware" to "Required Hardware"<br>Table 2: Changed "Caution Tag Printer" to "Zebra Printer"<br>Windows Updates: Reworded second paragraph for clarity.<br>Appendix A Troubleshooting: Changed to a document section called Troubleshooting. Also updated references to this section.<br>VBECS Exception Logging: Reworded first paragraph and added information to steps for clarity.<br>Performance: Removed the statement "The VBECS team will rely on VA Product Support to suggest network performance improvements."<br>Appendix E Data Center Instructions: Reworded Windows Updates section for clarity.<br>Global: Updated "EPS (Enterprise Product Support)" and CPS (Clinical Product Support) references to "VA Product Support"<br>Periodic Maintenance Checks, changed the Firmware Update Frequency to As needed.<br>Periodic Maintenance Checks, changed the Firmware Update Additional Notes to match the notes for Windows Updates.<br>Periodic Maintenance Checks, Changed the VBECS Updates Additional Notes to say "Forum informational patch messages when VBECS updates are tested and approved for installation.<br>Firmware Updates section, made consistent with the Periodic Maintenance Checks table. | BBM team |

| Date | Revision | Description | Author |
|---|---|---|---|
| | | Narrative text below Figure 74: Crystal Reports Message, changed “the next version” to “a future release”<br>VBECS Build Version Numbers section, reworded the last two sentences.<br>Appendix E: Data Center Instructions, Purpose, first sentence, changed “me” to “be”.<br>Installation Time Tasks, Complete the Checklists and Password List, changed Appendix B: “Server Hardware Checklist”, to “Blood Bank Hardware Checklist”.<br>Installation Time Tasks, Complete the Checklists and Password List, changed Appendix I to Appendix H. | |
| 4-22-09 | 4.0 | Updated guide to address comments from Clinical Product Support (CPS) review:<br>Configure Interfaces, Configure VistaLink Parameters: updated step 3.<br>Configure Interfaces, Configure CPRS HL7 Interface Parameters: updated step 2 and 3.<br>Configure Interfaces, Configure Patient Update HL7 Interface Parameters: updated step 3.<br>Configure Interfaces, Configure Patient Merge HL7 Interface Parameters: updated step 3.External Interfaces section: Updated the HL7 Service section to include VistALink listener updates.<br>Configure Interfaces, Configure VistALink Parameters, step 3, added third note. | BBM team |
| 5-12-09 | 5.0 | Updated guide to address comments from Clinical Product Support (CPS) review:<br>Reconfiguring the VBECS HL7 Multi Listener and VistALink Services section: Inserted the national port numbers into the .config file examples. Created instructions specific to test and production with the proper port numbers referenced. | BBM team |

# Table of Contents

This page intentionally left blank.

# Introduction

The main purpose of the VistA Blood Establishment Computer Software (VBECS) is to automate the daily processing of blood inventory and patient transfusions in a hospital transfusion service.

 *Unauthorized access or misuse of this system and/or its data is a federal crime. Use of all data must be in accordance with VA security and privacy policies.*

 *Do not change the system! The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations. Adding to or updating VBECS software without permission is prohibited.*

 *Changes to the system configuration must be documented with screen captures and kept with the installation record.*

## *Related Manuals and Reference Materials*

- *Health Level Seven Implementation Support Guide for HL7 Standard Version 2.3.1*, Message & Interface Services (M&IS), VHA OI - Health Systems Design & Development Web site (©1999).
- *Kernel Systems Manual Version 8.0*, Chapter 1: Sign-On Security/User Interface, pp. 13–20.
- "Locking Down Windows Server 2003 Terminal Server Sessions," Microsoft Web site (October 29, 2003).
- *National Software Package Distribution*, SOP 196-5.
- *Release of Patches*, SOP 196-8.
- *VBECS Application Interfacing Support Software Installation and User Configuration Guide.*
- *VistA Blood Establishment Computer Software (VBECS) Installation Guide.*
- *VistA Blood Establishment Computer Software (VBECS) User Guide.*
- *VistALink Version 1.0 Developer-System Manager Manual*, Chapter 6: Security Management, pp. 34–35.
- *Windows Server 2003 Security Guide 2.1*, Microsoft Corporation (May 8, 2006).

This page intentionally left blank.

# How This Technical Manual-Security Guide Is Organized

Outlined text is used throughout the guide to highlight warnings, limitations, and cautions:

 *Warnings, limitations, cautions*

## Terms

For consistency and space considerations, the pronouns "he," "him," and "his" are used as pronouns of indeterminate gender equally applicable to males and females.

In many instances, a user may scan a barcode or enter data manually (by typing). The term "enter" is used throughout this guide to mean "enter manually."

See the Glossary for definitions of other terms and acronyms used in this guide.

## Figures and Tables

If you refer to figures and tables from the technical manual-security guide in your local policy and procedure documents, you may wish to use their titles only, without figure or table numbers: as the technical manual-security guide is updated, those numbers may change.

## Screen Shots

Because VBECS is a medical device, screen shots must be captured at various points throughout the technical manual-security guide to meet FDA requirements for objective evidence and documentation. A  (camera) at the beginning of each step that requires a screen capture will identify these points. For more information, see Appendix A: Instructions for Capturing Screen Shots.

## Appendices

The appendices contain truth tables and other materials for reference.

While pressing the Ctrl button, left click on a section name or page number in the table of contents to move to that section or page. The index does not incorporate this feature.

This page intentionally left blank.

# Remote Desktop Configuration

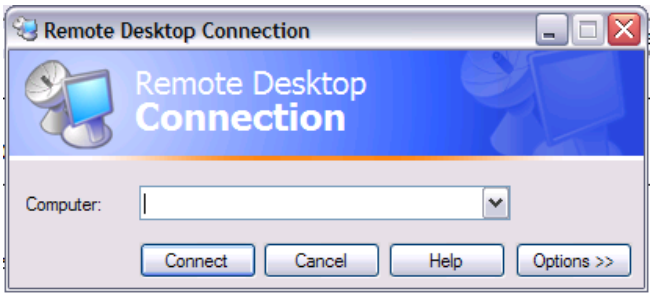
Configure the screen resolution, sound, and connection speed, and create a Remote Desktop Connection shortcut on each VBECS workstation.

## *Screen Resolution*

To set the screen resolution:

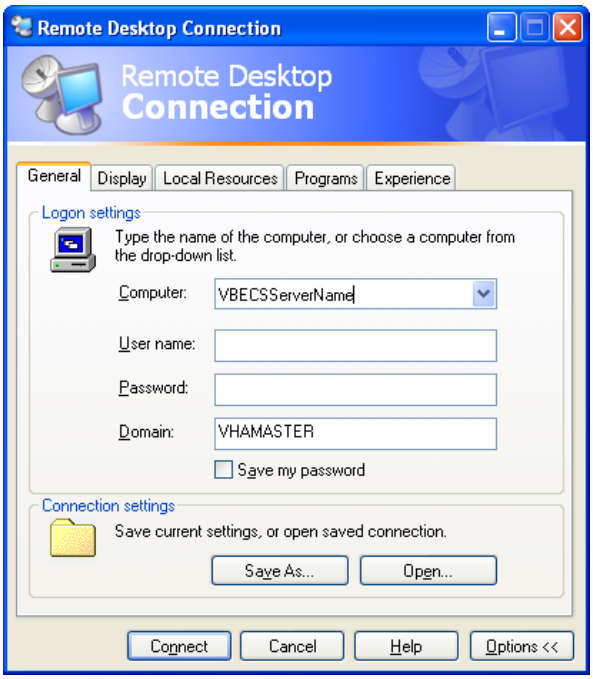
1) Double click (the **Remote Desktop Connection icon**).
2) Click **Options** (Figure 1).

**Figure 1: Remote Desktop Connection Options**



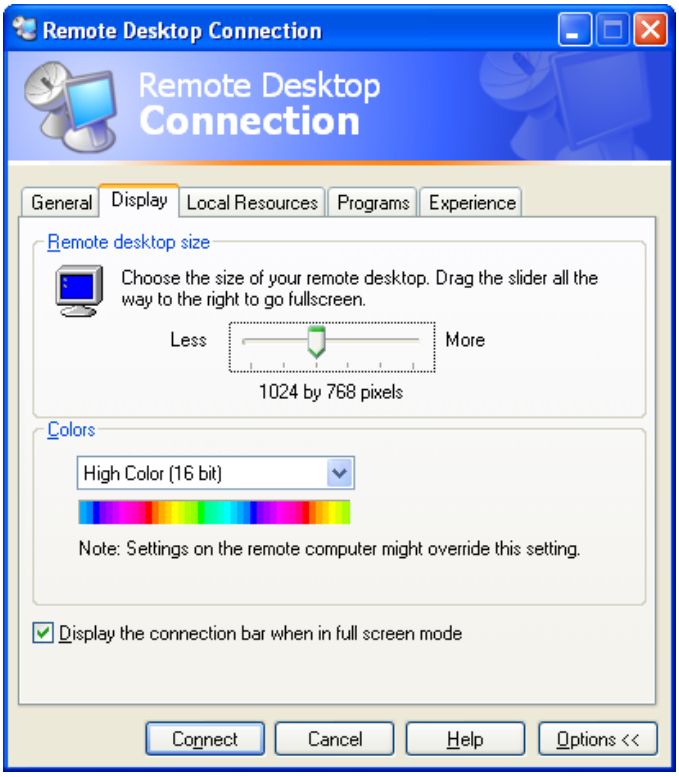

3) Click the **General** tab (Figure 2).
4) Enter the VBECS server cluster name or cluster IP address in the Computer field. Enter **VHAMASTER** in the Domain field. Do not enter a user name or password.

**Figure 2: General Tab: Computer and Domain**



5) Click the **Display** tab (Figure 3).
6) Click, hold, and slide the pointer to a screen resolution of 1024 by 768 pixels.

**Figure 3: Display Tab**



## *Sound*

To enable sound:

1) Click the **Local Resources** tab (Figure 4).
2) Select **Bring to this computer** from the Remote computer sound drop-down list.

*Failure to properly configure the sound disables audible alerts throughout VBECS.*

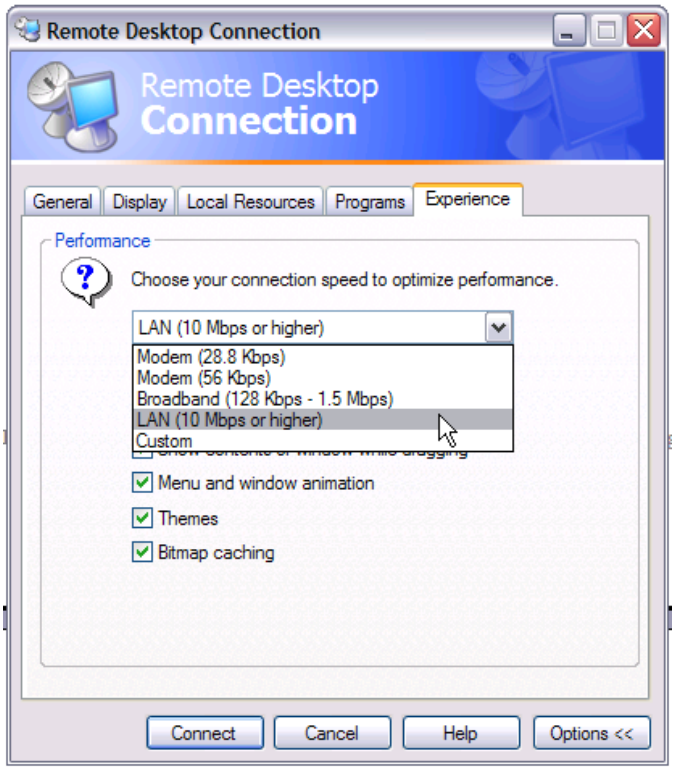
**Figure 4: Computer Sound**

## *Connection Speed*

To set the connection speed:

1) Click the **Experience** tab (Figure 5).
2) Select **LAN (10 Mbps or higher)** from the **Choose your connection speed to optimize performance** drop-down list.

**Figure 5: Connection Speed**

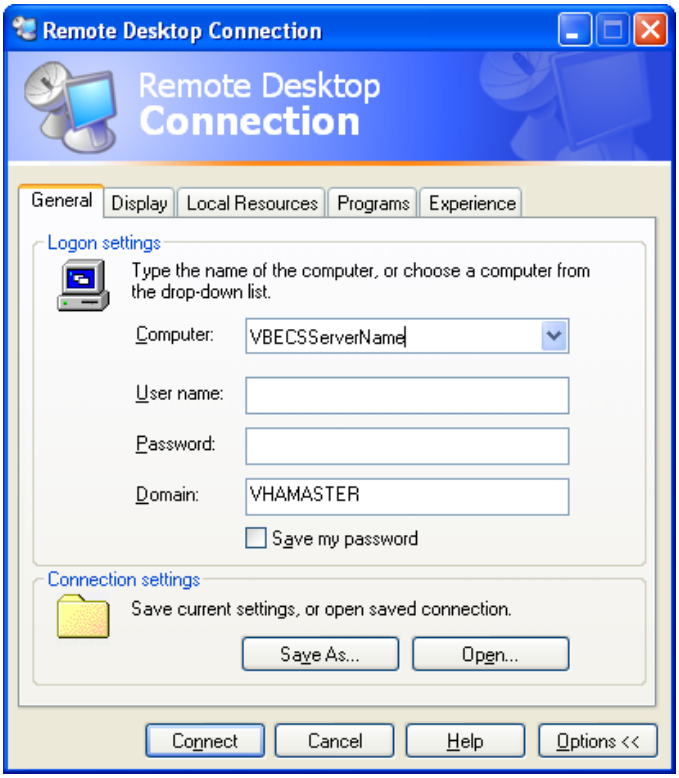


## *Save Settings*

To save the settings:

1) Click the **General** tab (Figure 6).
2) Click **Save As**.

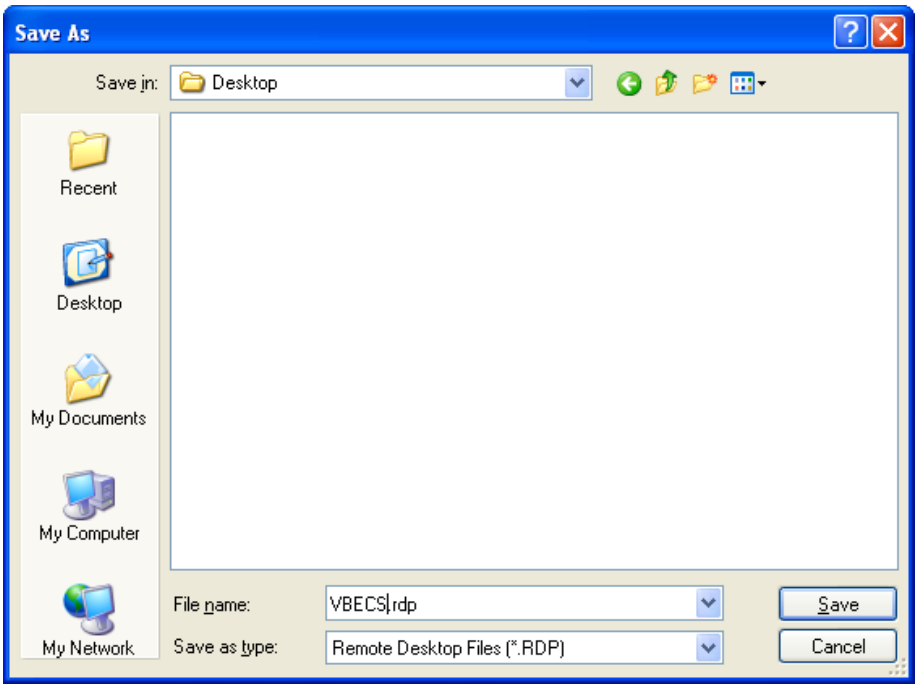
**Figure 6: General Tab: Save**



## *Create a Remote Desktop Connection Shortcut for VBECS*

1) To create a Remote Desktop Connection shortcut for VBECS (Figure 7), save the file as VBECS.rdp in the All Users, Desktop folder.

**Figure 7: Remote Desktop Connection Shortcut for VBECS**




2) Double click the shortcut to launch the remote desktop connection to VBECS.
3) The Windows start-up sound confirms that the sound functions.

# Server Hardware and System Configuration

The VBECS application requires that hardware and system software serve five users in a standard configuration and up to 25 users in an integrated Veterans Integrated Service Network (VISN) environment.

The System Schematic diagram (Figure 14) describes the major system components: a Windows 2003 Server system (the execution environment for the VBECS application) and Windows XP workstations, with which the user will access the VBECS application using Windows Terminal Services [Remote Desktop Protocol (RDP)]. The VBECS server will also communicate with and exchange information with VistA applications through messages formatted using Extensible Markup Language (XML) and Health Level Seven (HL7) over Transmission Control Protocol/Internet Protocol (TCP/IP) networking.

## *Server and Shared Array discs*

### Server Disc Configuration

Each VBECS server has two discs in a RAID 1 (mirroring) configuration (Figure 8). This means that if one disc fails, the server will continue to run normally.

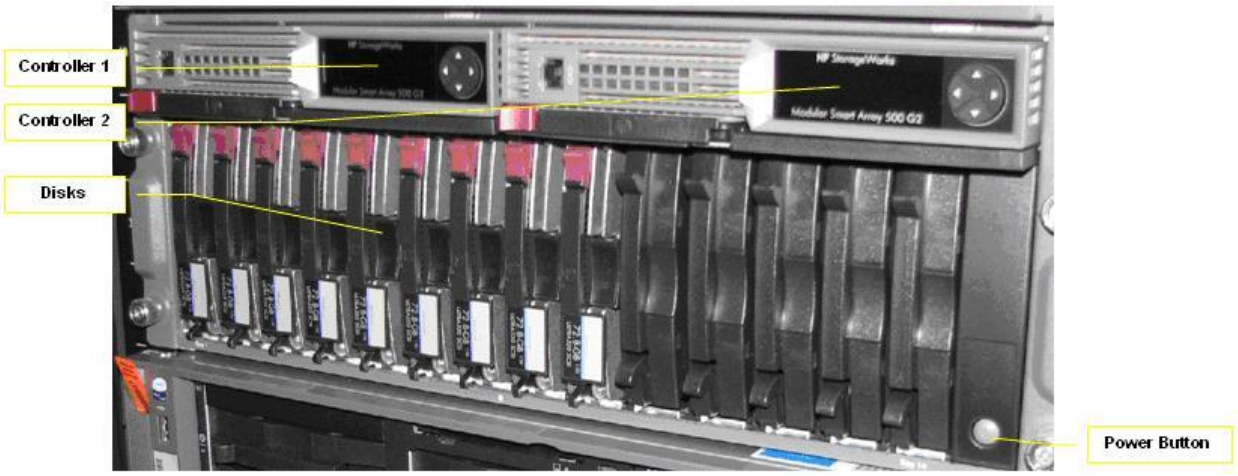
**Figure 8: Server discs**

### Shared Array Configuration

The shared disk array consists of nine disks (Figure 9).

- The first four discs are used to store VBECS specific data. These are configured as RAID 5.
- The fifth disc is a hot spare. It can be used if one of the other discs fails. Note that the LED on it will be off.
- Discs 6 and 7 are for log storage. These are configured as RAID 1.
- Discs 8 and 9 are for cluster support. These are configured as RAID 1.

**Figure 9: Shared array**




## Replacing a disc

All discs in the system, both server and array, are hot swappable. This means that if a disc should fail, it can be replaced without powering down the system or disrupting users. Simply remove the failing disc and replace it with a new one. It will take a couple of minutes to rebuild. For more information on monitoring and viewing disk health, please see the HP Array Diagnostic Utility section.

# *Printers*

## Laser Printer

A laser printer capable of printing 8.5" x 11" sheets may be used. Set it up as described in *VistA Blood Establishment Computer Software (VBECS) Installation Guide*.

## Label Printer

VBECS is configured to work only with Zebra printers: VBECS uses Zebra printing language to communicate with the printer. Other requirements:

- Ethernet connectivity: the label printer must have an Ethernet card.
- Must print on 4" x 4" label stock
- Must print at 300DPI

Prior to configuring the label printer, load the ribbon and label stock and ensure that the printer is on. If the printer does not display PRINTER READY, there is a problem that must be resolved before proceeding. Refer to the Zebra user guide or printer CD for more information.

### Set the IP Address on the Printer

1) Press **SETUP/EXIT** to access the configuration menus.
2) Press + or – to scroll through the configuration menu option. Stop when IP PROTOCOL is displayed and press **SELECT**. If there is a prompt for a password, press – to change positions and + to change numbers. Enter **1234**. Press **SELECT**.
3) Press + to select PERMANENT. Press **SELECT**. The IP address is configured to be static.

4) Press + to navigate to the IP ADDRESS menu option. Press **SELECT**.
5) Press + or – to change numbers (as in Step 2) to enter the IP address specified in the Configuration Checklist. Press **SELECT**.
6) Press **SETUP/EXIT** to save the new configuration. PERMANENT is displayed. Press **SETUP/EXIT** to save the changes.

### Test the Printer

To print a label, press and hold the Network Configuration button (on the back of the printer just above the Ethernet socket) until the DATA LED on the front of the printer blinks. Retain the test label for validation records. If the printer configuration on the label print is blank or faint or it is printing off center, adjust the settings.

### Adjust Label Darkness

If the printer configuration on the label print is blank or faint, adjust the darkness:

1) Press **SETUP/EXIT**. Press + or – until DARKNESS is displayed. Press **SELECT**.
2) Press + to adjust the darkness to a higher number. Press **SELECT**. Move up in small increments: setting the printer to a setting that is too dark may compromise the quality of the labels.
3) Repeat these steps to retest the printer.
4) If parts of the label are cut off, adjust the X and Y offsets.
5) Press **SETUP/EXIT** twice to permanently change the setting.

### Adjust Label Offsets

If the printer is printing off center, adjust the X and Y offsets:

1) Press **SETUP/EXIT**. Press + or – until LABEL TOP (if vertical alignment is not correct) or LEFT POSITION (if horizontal alignment is not correct) is displayed. Press **SELECT**.
2) Press + or – to adjust the alignment to a higher number. Press + in the LABEL TOP menu to move the printing down on the label. Press + in the LEFT POSITION menu to move the printing to the right on the label.
3) Press **SELECT**. Adjust in small increments until the label is centered on the label stock.
4) Press **SETUP/EXIT** twice to permanently change the setting.

## *Scanners*

Scanners used with VBECS must be able to scan Codabar, ISBT 128, and PDF-417 barcodes. To configure a scanner:

1) Connect the scanner to the workstation.
2) To configure a Hand Held 4600 barcode scanner, scan the barcode in Figure 10. Repeat for all scanners.

**Figure 10: Configure a Barcode Scanner**

3) To test the scanner, open Notepad. Print and scan the barcodes in Figure 11, Figure 12, and Figure 13. The Codabar and ISBT barcodes must scan as "~123456789"; the PDF 417 must scan as "~Testing."
4) Save and print the Notepad file for validation records.

**Figure 11: Codabar**

**Figure 12: ISBT 128**

**Figure 13: PDF 417**

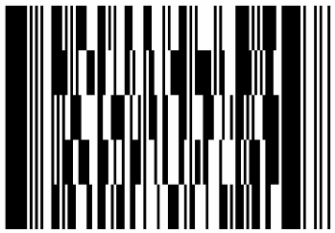
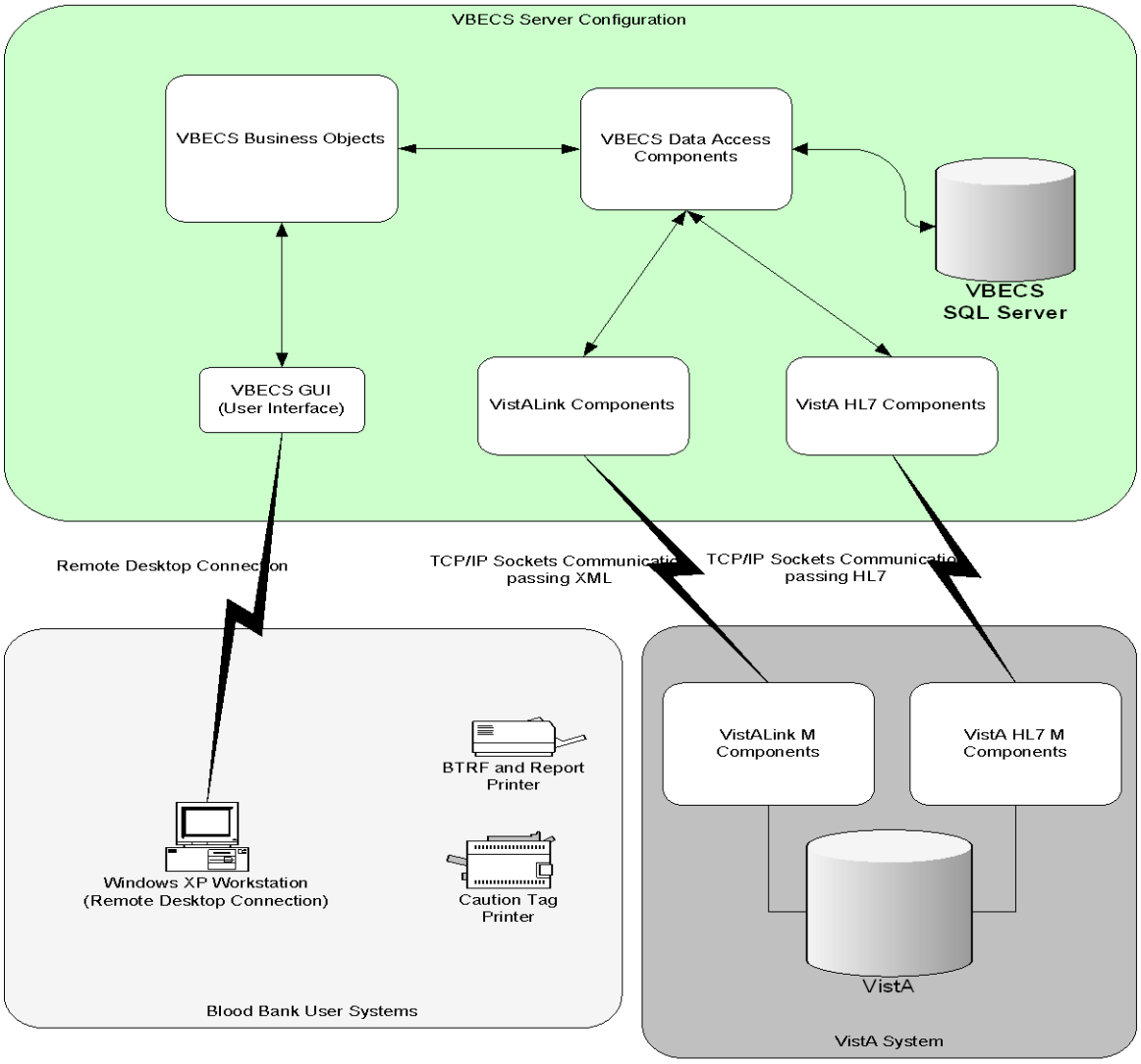


**Figure 14: System Schematic**



## Server Configuration

*The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations.*

**Table 1: Server Configuration**

| Hardware | Clustered Database Server (two identical systems) |
|---|---|
| Processor | Multiple processors (2–4 processors) Pentium 4 Xeon 2.0 GHz processors (or greater) with 512kb level 1 cache |
| Memory | 2-gigabyte (or greater) main storage (RAM) |
| Storage | Shared Storage Controller Unit. Disk configuration: 8 hot swappable SCSI hard drives (minimum 10,000 RPM) The system drives require 18 gigabytes (or greater) storage capacity. The application data drives require 36 gigabytes; log volume and historical data drives require 72 gigabytes (or greater) storage capacity. |
| Operating System | Microsoft Windows 2003 Server Enterprise with Microsoft Clustering Services providing failover data-device sharing |
| Network Controller | Multiple 10/100 network cards configured to provide fallback in event of failure. |
| Power Supply | Primary and secondary (redundant) power supply to server chassis and an uninterruptible power source (UPS) |
| Backup | Internal tape backup with software |

This configuration is designed to promote 24/7 availability and use of the application. A clustered database server configuration will provide near immediate failover if one node of the server fails. Multiple processors will provide for more efficient processing of database access requests and operating system processes.

Dual power supply and UPS will ensure that the machine will not lose operating power. The disk storage configuration will allow the server disks to be shadowed: if a main disk fails, the shadow disk will automatically continue system operation until the primary disk is replaced. Hot swappable disk drives can be replaced without shutting down the server. Internal tape backup on the application data disk will allow an image of the application data to be restored to another machine if the server is damaged.

## Required Hardware

**Table 2: Required Hardware**

| Hardware | Description |
|---|---|
| Zebra Printer | Zebra printer capable of producing barcoded labels (network capable) |
| Barcode Scanner | Symbol Model LS4006i barcode scanner for each workstation |
| Report Printer | Laser printer or comparable with sufficient speed to handle high-volume reports (network capable) |

## Workstation Configuration

**Table 3: Workstation Configuration**

| Hardware | Description |
|---|---|
| Processor | Suitable for Windows XP |
| Memory | 256 megabytes (or greater) main storage (RAM) |
| Monitor | 17" monitor or greater |
| Video | Video card capable of displaying minimum of 16-bit color at 800 x 600 resolution |
| Disk Storage | 9 gigabytes (minimum) |
| Operating System | Microsoft Windows XP Professional with Microsoft Terminal Services Client |
| Network Controller | 10/100 network card |
| Input Devices | U.S. 101-key keyboard, mouse |
| Audio | Sound card and speakers (may be internal) |

## Off-the-Shelf Software Requirements

 *Do not upgrade, change, or add software to the VBECS server: this may compromise the integrity of VBECS.*

**Table 4: Off-the-Shelf Software Requirements**

| Software | Description |
|---|---|
| .NET Framework | Version 1.1 |
| SQL Server | SQL Server 2000 Enterprise Edition |
| Crystal Reports | Crystal Reports .NET |
| Backup software | VERITAS Backup Exec Version 10.0 |
| McAfee VirusScan | Version 8.0 |

This page intentionally left blank.

# Implementation and Maintenance

*The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations.*

## *Periodic Maintenance Checks*

The configuration that enables audible alerts has client and server sides. Check client workstations periodically to ensure that end users did not turn off the audible alerts. Ensure that the client workstation configuration matches the configuration in Hardware Specifications and Settings.

The system will fail to function as intended when maintenance checks are not performed or are performed incorrectly. Follow all instructions in the *VistA Blood Establishment Computer Software (VBECS) Installation Guide* for configuration. Check Microsoft Operations Manager (MOM) alerts daily. Local policy must create a schedule to check client configuration settings.

The following checklist details additional required server maintenance tasks:

| Description | Frequency | Additional Notes |
|---|---|---|
| Backup tape rotation | Daily | If using Backup Exec, backups automatically occur every morning per the time specified in the VBECS Installation Guide. Refer to local policy for data retention and offsite storage requirements. |
| Database Integrity Report | Weekly | Check the DatabaseIntegrityCheck.log report weekly. Open the file as described in Database Integrity. Scroll to the bottom of the file and ensure that the file includes "CHECKDB found 0 allocation errors and 0 consistency errors in the database <database>." If the log file lists errors, file a Remedy ticket describing the errors found. |
| Windows Updates | 2nd Tuesday of the month | Forum informational patch messages are posted when the updates have been tested and approved for installation. |
| Firmware Updates | As needed | Forum informational patch messages are posted when the updates have been tested and approved for installation. |
| VBECS Updates | As needed | Forum informational patch messages when VBECS updates are tested and approved for installation. |

## *Windows Updates*

If your servers reside at a data center that has its own update distribution system, please refer to Appendix E: Data Center Instructions.

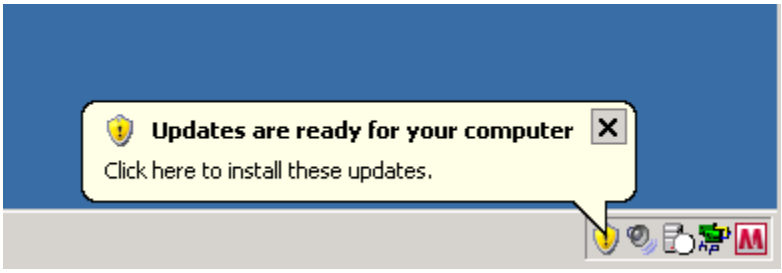
The VBECS development team must test every Microsoft Windows update. Once the development team is satisfied that the update causes no adverse effects, they will notify sites that there are Windows or Firmware updates. A VistA information patch in the VBEC namespace will be created by the VBECS team each time an update is available describing where to obtain the update and how to apply it. The patch will be released to customers by VA Product Support.

Updates are approved with Windows Software Update Service. Approved updates will be downloaded to your servers automatically. However, a server administrator must install the updates locally.

VA Product Support will notify the sites of updates required for installation.

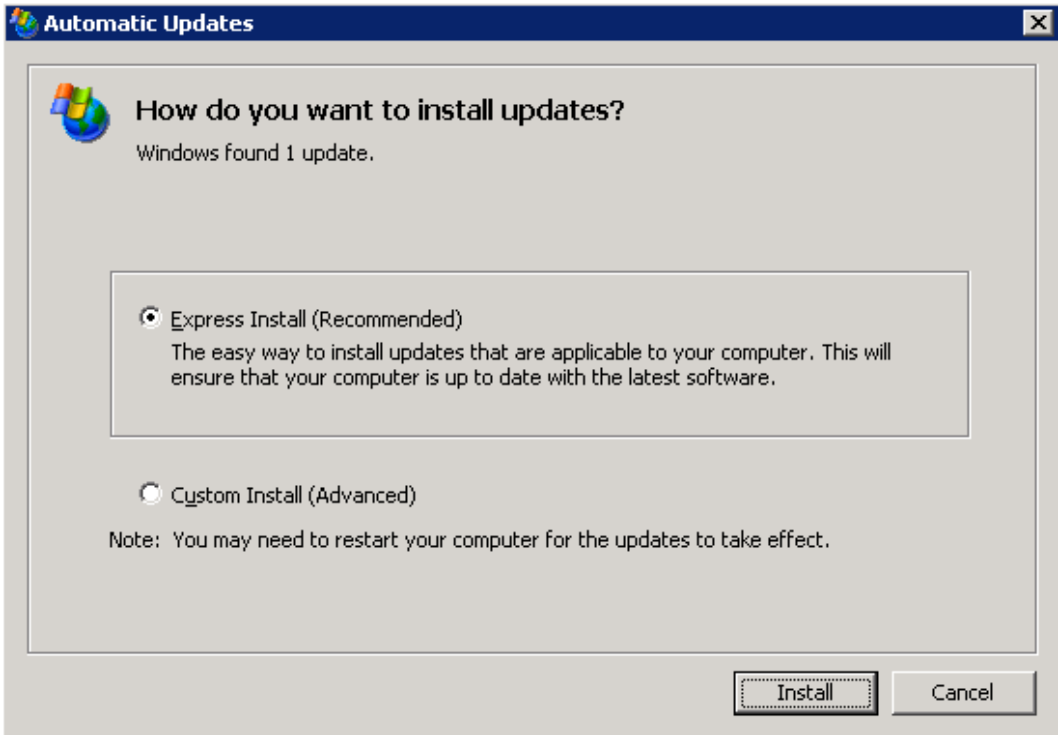
1) Since most updates require a reboot, coordinate a time with the blood bank manager to apply the updates.
2) At the agreed upon time, log onto the first server as a user with administrative privileges.
3) A shield shaped icon will appear in the System Tray (lower right corner of desktop). Click on it (Figure 15).

**Figure 15: Windows Software Update Notification**




4) Leave **Express Install** selected. Click **Install** (Figure 16).

**Figure 16: Example of Install Updates**



5) When the update process is complete, you may be prompted to reboot. If so, reboot the server at this time.
6) After the server completely reboots, repeat this process on the second server.

## ePolicy and Virus Definitions

The VBECS development team must test virus definitions before they are applied to the servers. The VBECS development team will send the virus definitions: do not apply virus definitions locally.

*Do not change the system! The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations. Adding to or updating VBECS software without permission is prohibited.*

## Commonly Used System Rules

This section includes system rules that apply to several or all options.

- Only one instance of Configure Interfaces may run at a time.
- VBECS captures changes to verified data for inclusion in the Audit Trail Report.
- VBECS protects application data through encapsulation. Encapsulation promotes data security by hiding the implementation details.

*The dialogs defined in Configure Interfaces and Configure Divisions cannot run when VBECS is operational. VBECS cannot run when a dialog in these options is operational.*

## Firmware Updates

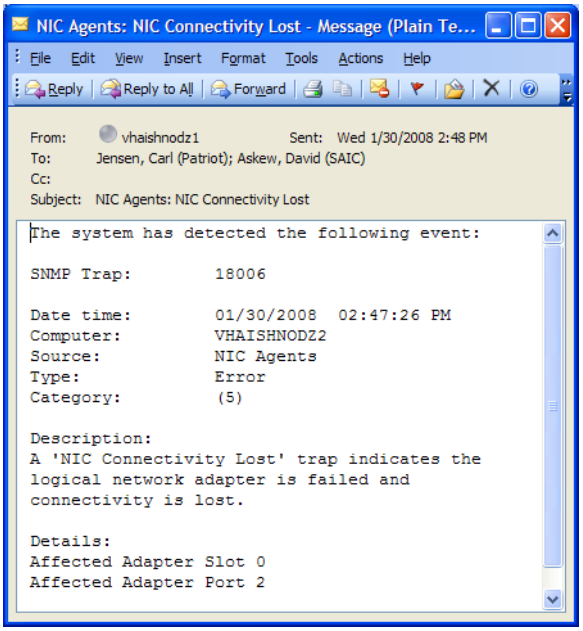
Forum informational patch messages are posted when the updates have been tested and approved for installation.

## *Hardware Utilities and Backup Exec Alerts*

### HP Event Notifier

Hardware alerts are generated with HP Event Notifier. Event Notifier will generate email alerts whenever a hardware failure occurs. Examples of hardware failures include, but are not limited to: controller, network interface card and fan failures. An example of a network interface card losing connectivity is displayed in Figure 17.

**Figure 17: Example of an email alert from Event Notifier**




When an alert is received, a server administrator should investigate the problem as soon as possible in order to prevent VBECS downtime. If necessary, contact HP support for assistance at: 800.633.2600.

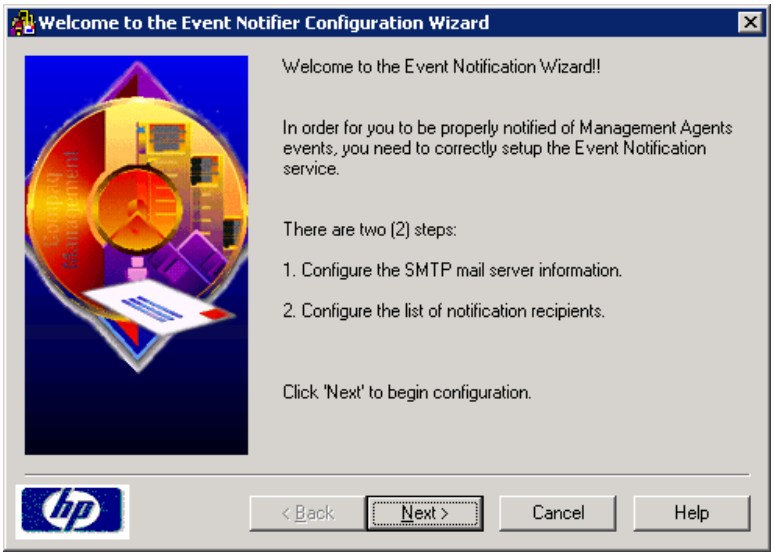
#### Configuring Event Notifier

To add or modify hardware alerts on servers, take the following steps:

1) Log into the server with administrative rights.
2) Click **Start**, **HP Management Agents**, **Event Notifier Config**.

3) Click **Next** (Figure 18).

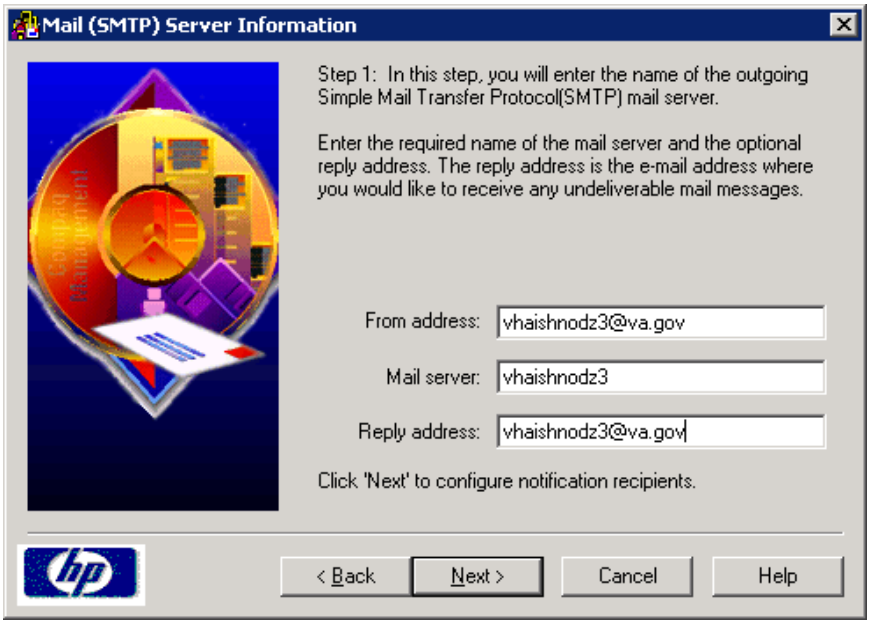
**Figure 18: Welcome screen**




4) Enter the following (Figure 19):
   - From address: <servername>@va.gov
   - Mail server: <servername>
   - Reply address: <servername>@va.gov

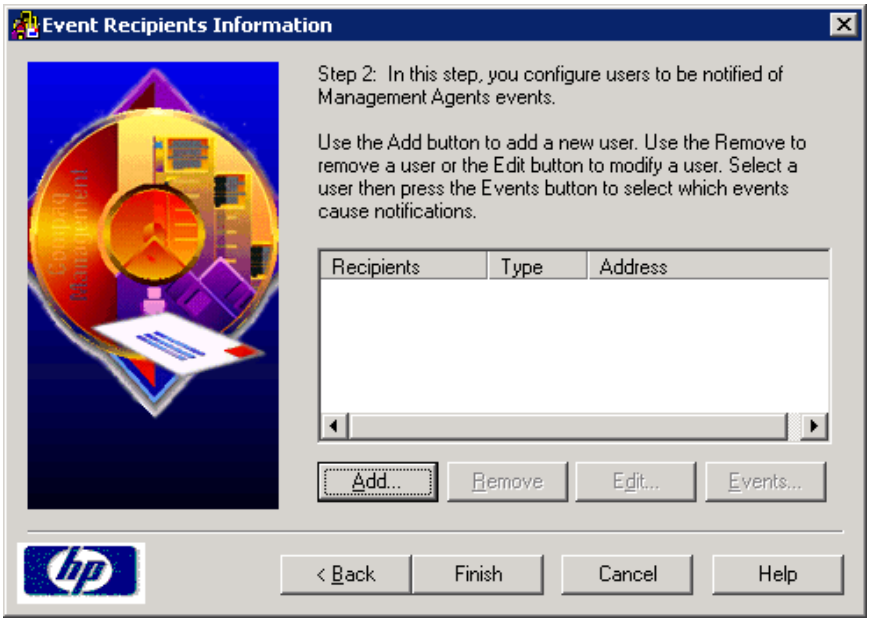
   Click **Next**.

**Figure 19: Example of SMTP configuration**



5) Click **Add** (Figure 20). Note that **Remove** or **Edit** can be used for modification and deletion of existing groups respectively.

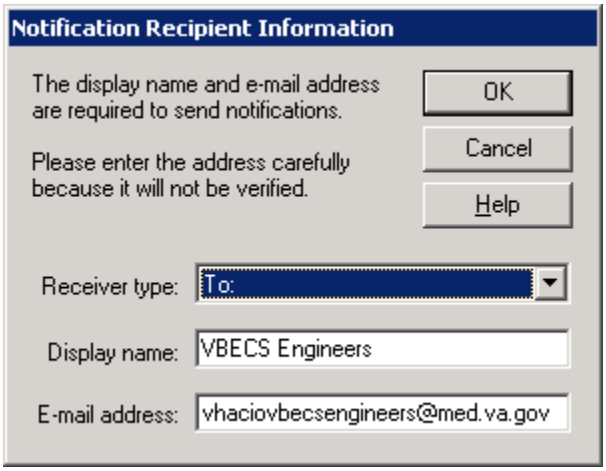
**Figure 20: Recipients**




6) Enter the following (Figure 21):
   - Display name: Arbitrary name that describes the email group being entered
   - E-mail address: Email group address of support personnel (Figure 21). Note: Use the support email address that was defined in the VBECS Installation Guide (Appendix E, Contact Information).

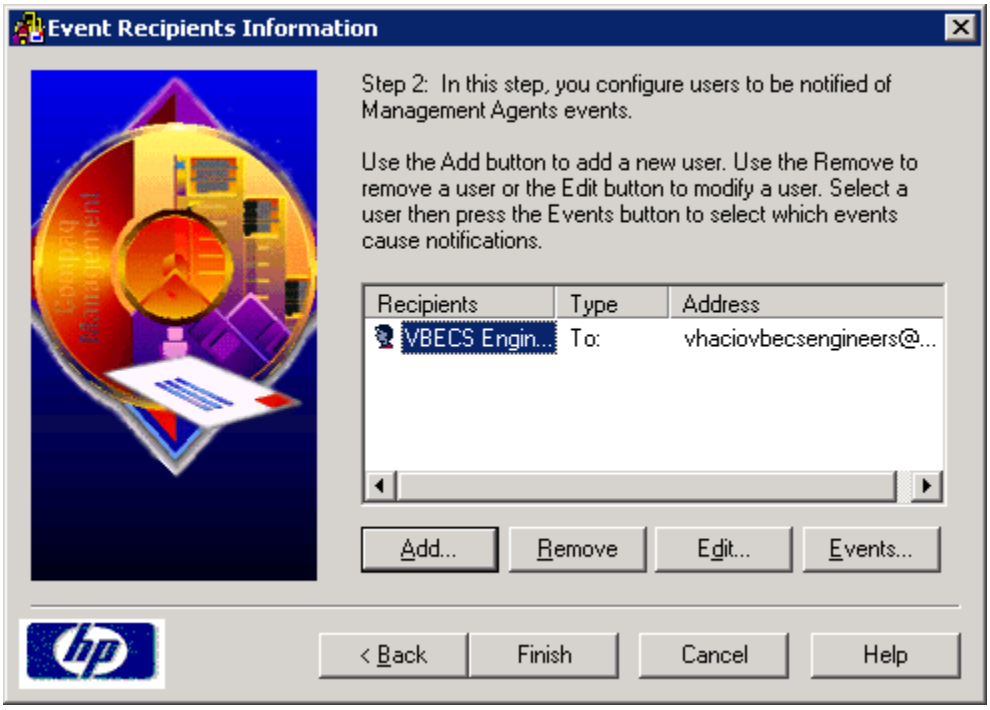
   Click **OK**.

**Figure 21: Example of Recipient Information**



7) Click **Finish** (Figure 22). Repeat these instructions on the other server.

**Figure 22: Done!**



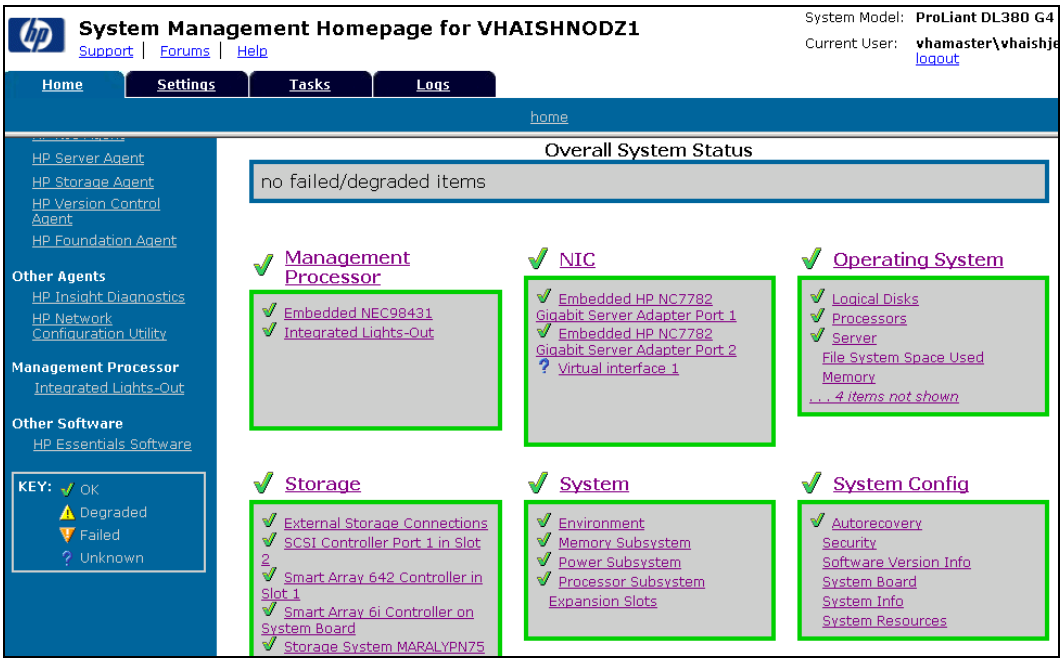

## HP System Utilities

There are several pre-installed utilities on the system that are useful when checking hardware health and diagnosing problems. All of these tools are launched from the **Start** menu and all require administrative rights. Please see HP documentation for specific information regarding further use of any of these tools.

### HP System Management Homepage

This is a tool that quickly lets the administrator see the status of all major components of the system including the shared array (Figure 23).

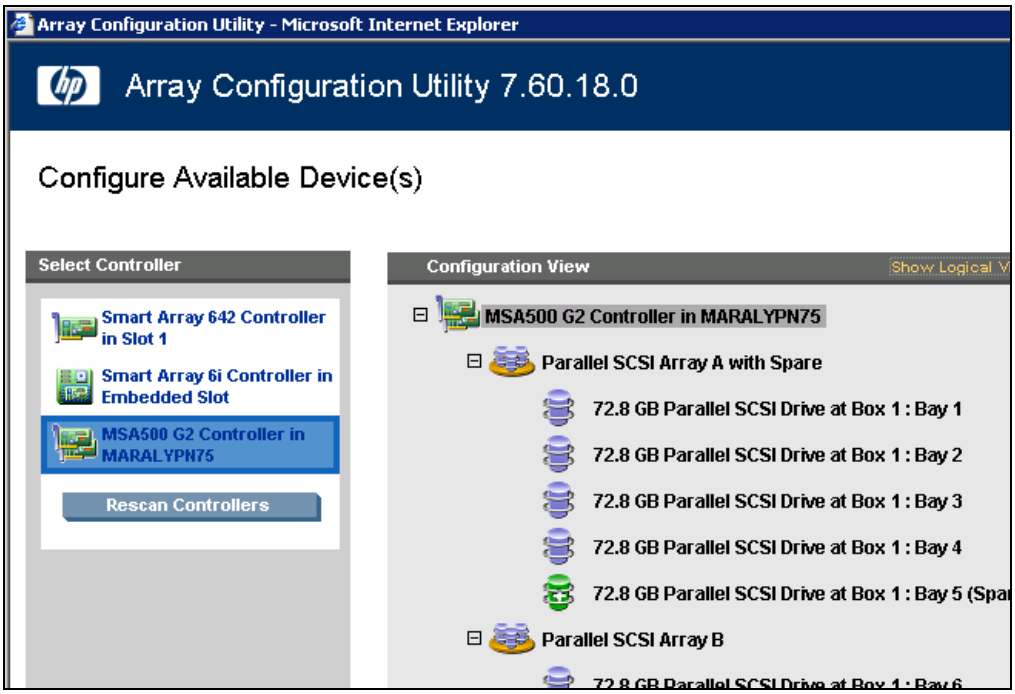
**Figure 23: System Management Homepage**



### HP Array Configuration Utility

This tool shows the state of discs, both server and shared array (Figure 24).

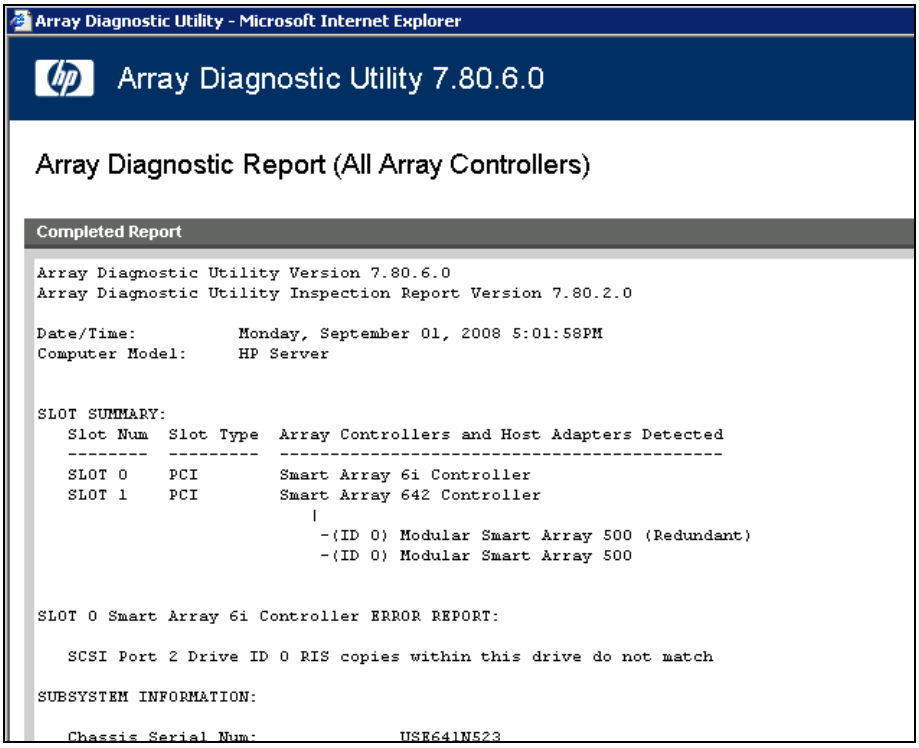
**Figure 24: Array Configuration Utility**



### HP Array Diagnostic Utility

This tool generates a report showing the status of disks, both server and shared array (Figure 25). It is useful for diagnosing disc problems.

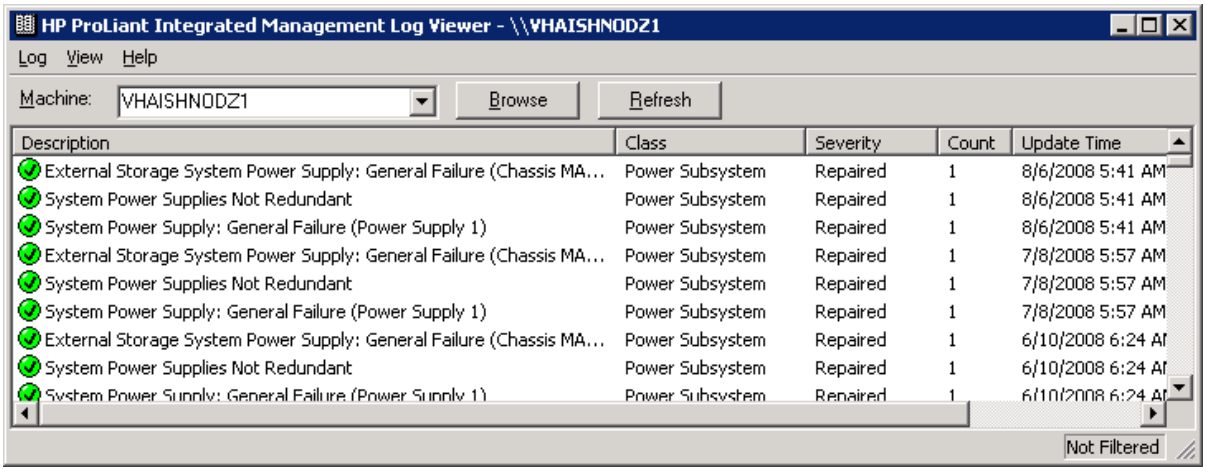
**Figure 25: Array Diagnostic Utility**




### HP ProLiant Integrated Log Viewer

All hardware related issues are logged here (Figure 26).

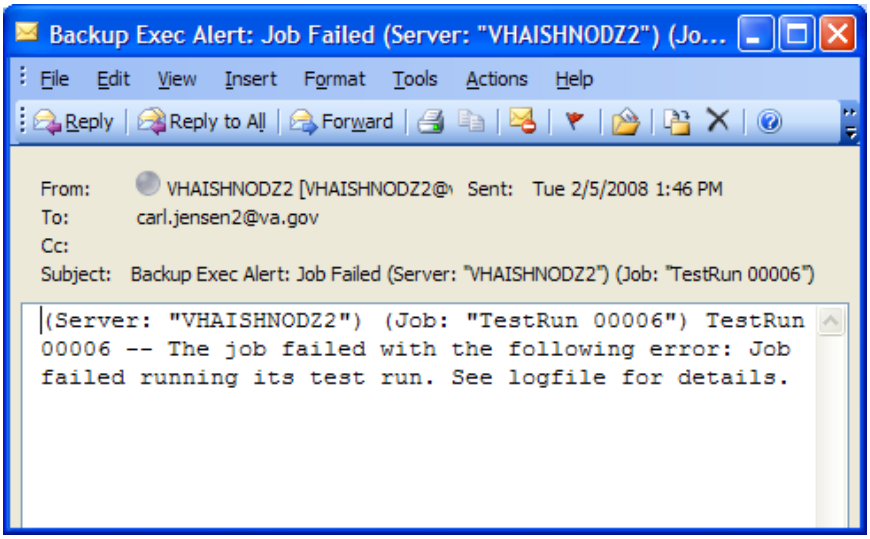
**Figure 26: HP ProLiant Integrated Log Viewer**



## Backup Exec Alerts

Backup Exec job failure alerts are sent by Backup Exec. Whenever the nightly job fails, an alert will be sent. An example of one of these alerts is displayed in the screen capture below (Figure 27).

**Figure 27: Example of an email alert from Backup Exec**




When an alert is received, a server administrator should investigate the problem as soon as possible in order to ensure proper data backup.

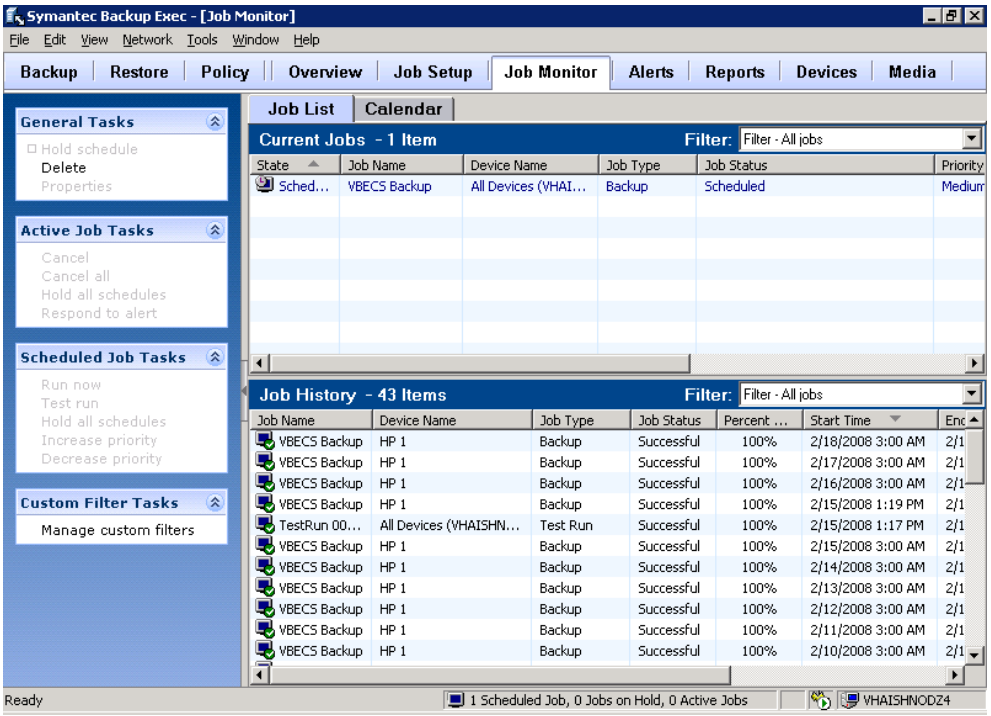
### Configure Backup Exec Alerts

To add or modify Backup Exec Alerts on servers, take the following steps:

1) Log into the server (not the cluster) that has Backup Exec installed with administrative rights.
2) Click **Start**, **All Programs**, **Symantec Backup Exec 10d for Windows Servers**

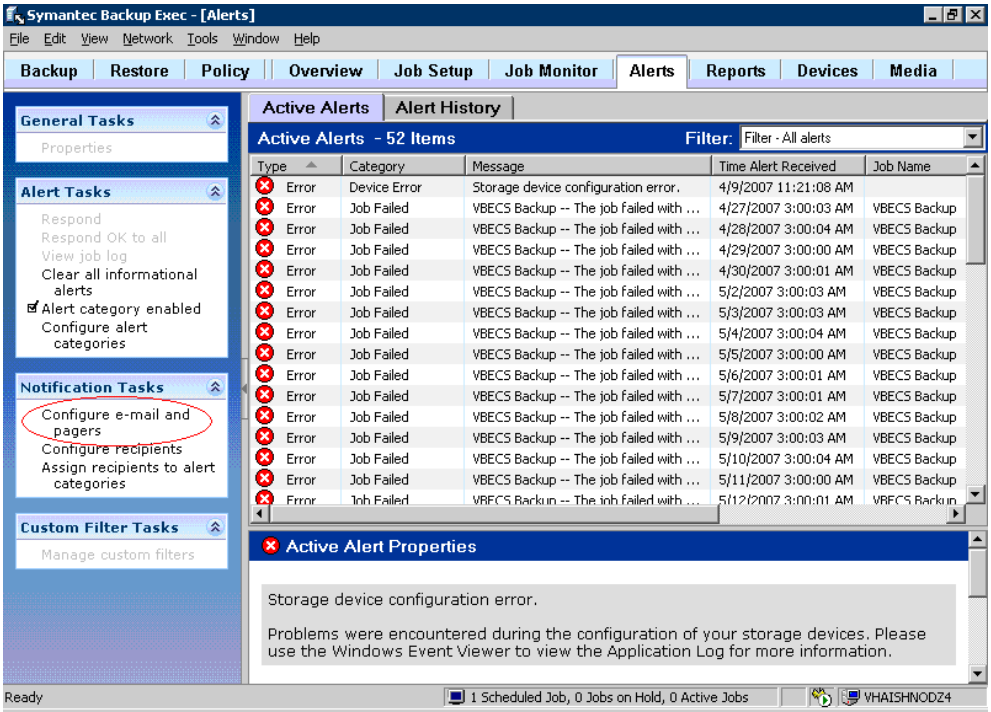
3) Click **Alerts** (Figure 28).

**Figure 28: Backup Exec main screen**




4) Click **Configure e-mail and pagers** (Figure 29).

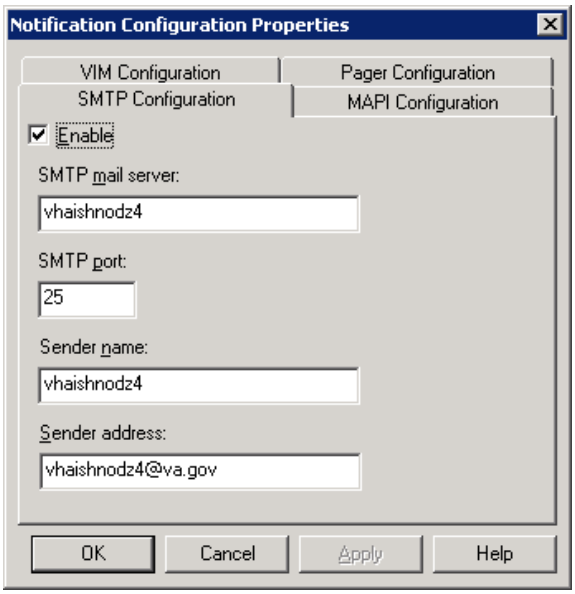
**Figure 29: Example of Alerts**



5) Enter the following (Figure 30):
   - Check the **Enable** box
   - SMTP mail server: <server name>
   - Sender name: <server name>
   - Sender address: <server name>

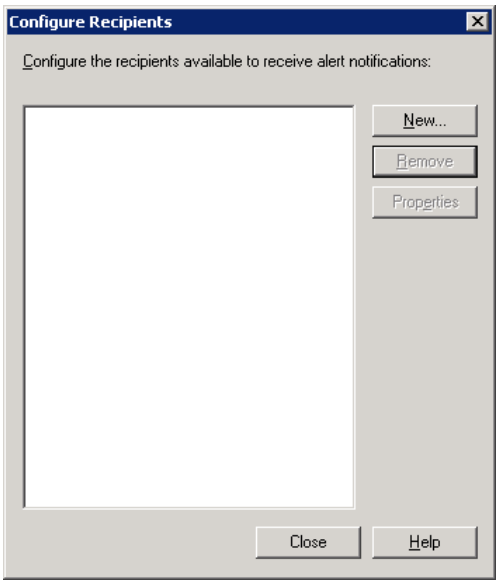
   Click **OK**.

**Figure 30: Example of SMTP Configuration**



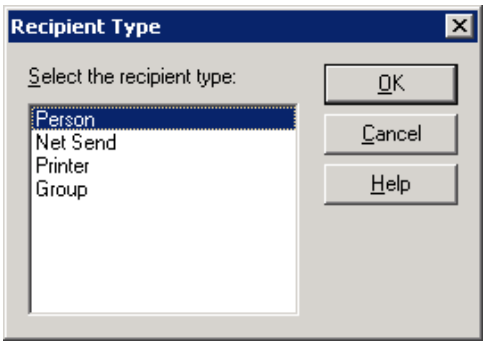

6) Click **Configure recipients** on the main Alerts screen. Click **New** (Figure 31). Note that **Remove** or **Properties** is used for deletion and modification of existing groups respectively.

**Figure 31: Configure Recipients**



7) Click **OK** to select Person (Figure 32).

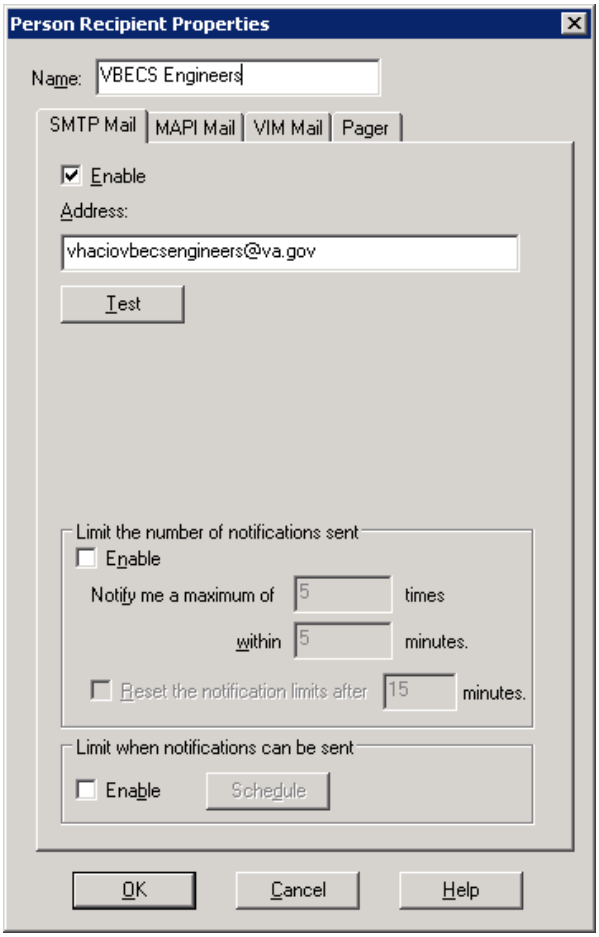
**Figure 32: Recipient Type**




8) Enter the following (Figure 33):
   - Name: Arbitrary name that describes the email group being entered
   - Check the **Enable** box
   - Address: Email group address of support personnel (Note: Use the support email address that was defined in the VBECS Installation Guide (Appendix E, Contact Information).

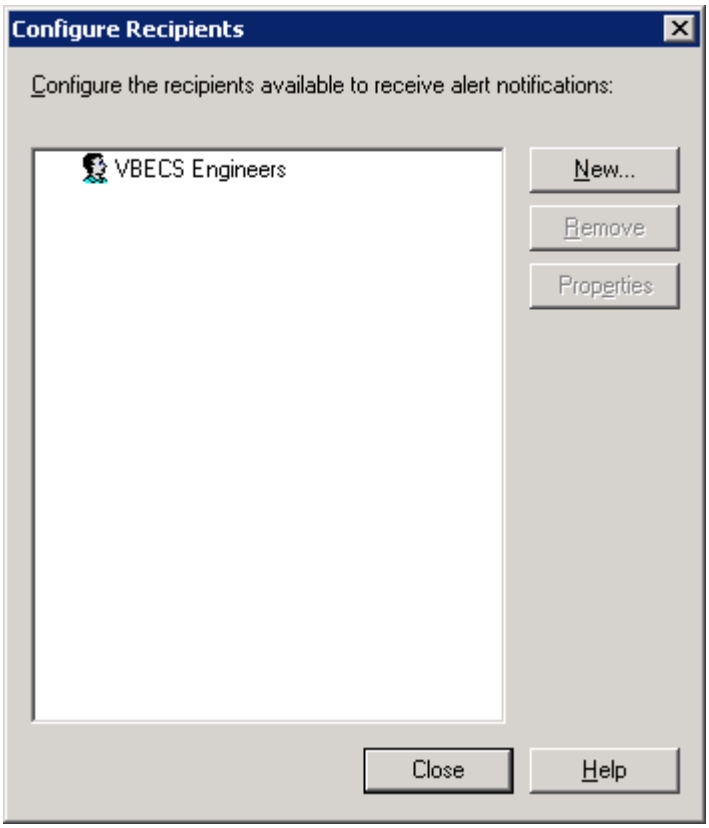
   Click **OK**.

**Figure 33: Example of Recipient Properties**



9) Click **Close** (Figure 34).

**Figure 34: Example of Configure Recipients**



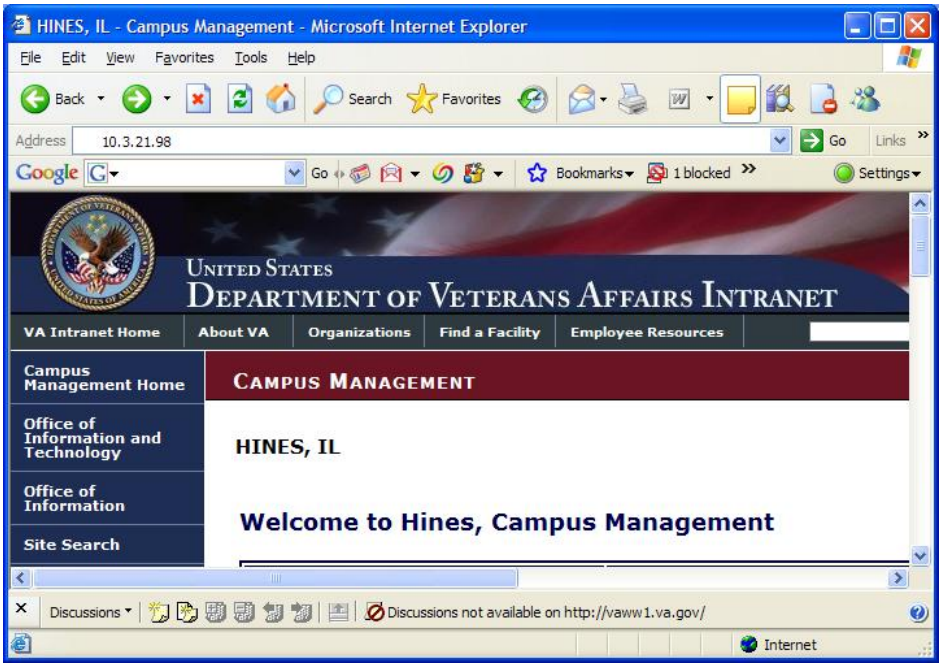

## *Integrated Lights Out*

Integrated Lights Out (iLO) is a separate hardware component of the server that allows for increased remote administrative capabilities via a separate network connection. For example, the server can be turned on and diagnostic information can be viewed through the iLO console. For instructions on installing iLO and defining users, please see Appendix L of the VBECS Installation Guide. This section assumes you have already executed those instructions.

## To access iLO

1) From any computer in the VA wide area network (WAN), launch a web browser and enter the iLO IP address of the server you would like to administer (Figure 35). Press **Enter**.

**Figure 35: Internet Explorer**

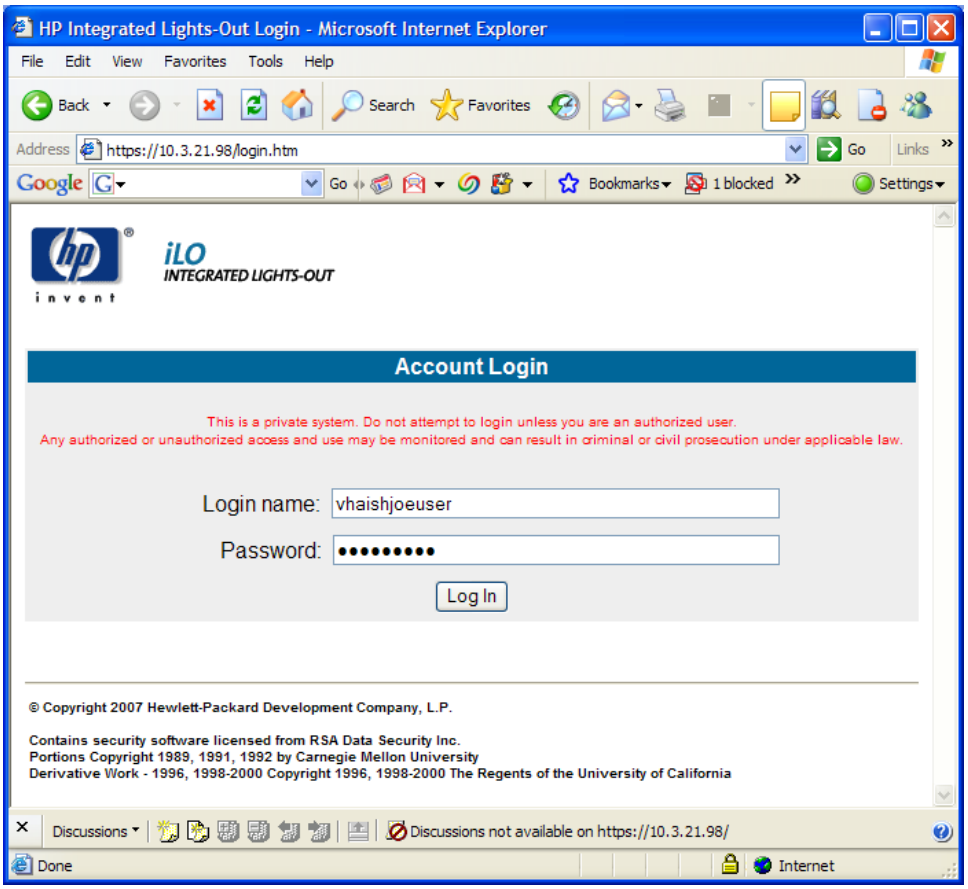



2) Click **Yes** to proceed (Figure 36).

**Figure 36: Security Alert**

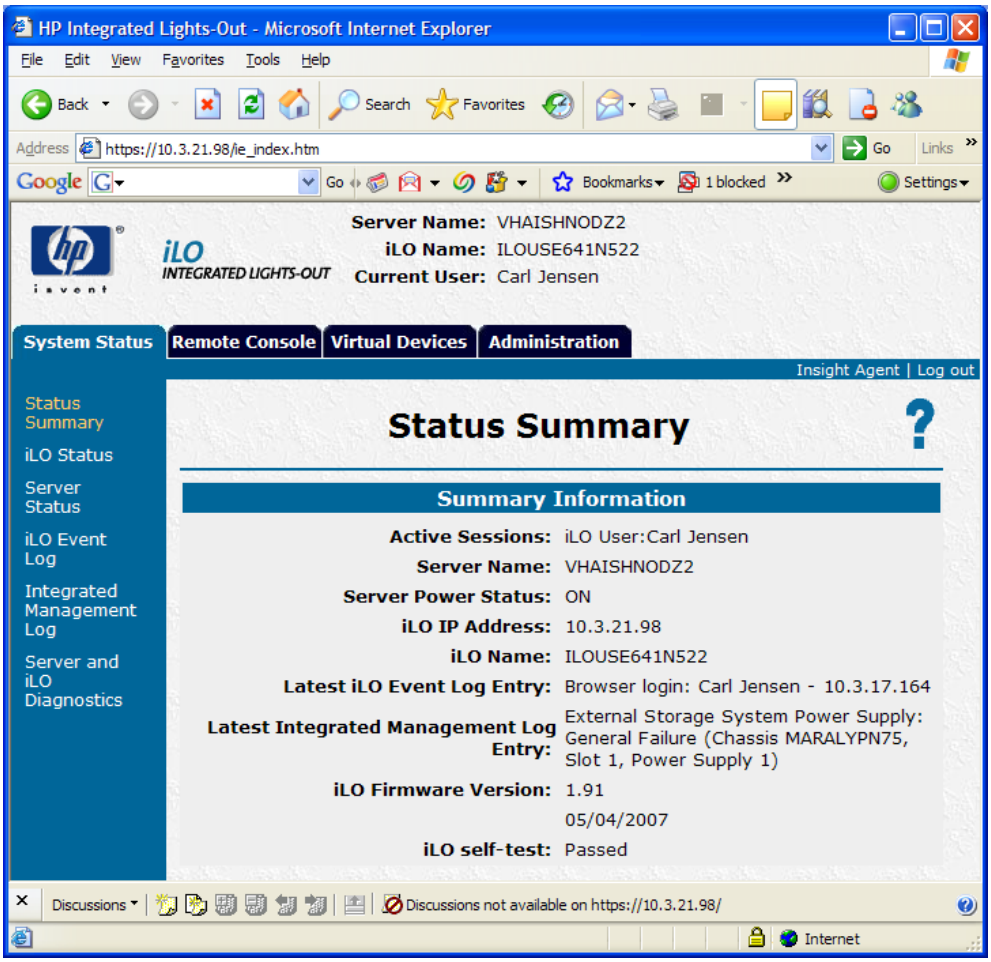
3) Enter your username and password and click **Log In** (Figure 37):

**Figure 37: Example of iLO Login**



4) The iLO summary page is displayed (Figure 38).

**Figure 38: iLO Summary page**




### System Status tab (Figure 38)

Brief explanation of iLO menu items:

- Status Summary: Basic iLO configuration
- iLO Status: Indicates current condition of iLO
- Server Status: Server configuration and status
- iLO Event Log: Events related to iLO
- Integrated Management Log: Log showing server events and error conditions
- Server and iLO Diagnostics: Results of automatic diagnostic tests

### Remote Console tab

Options in this tab are unavailable at this time.

### Virtual Devices tab (Figure 39)

Options in this tab allow you to accomplish tasks remotely that would normally require you to be at the server console:

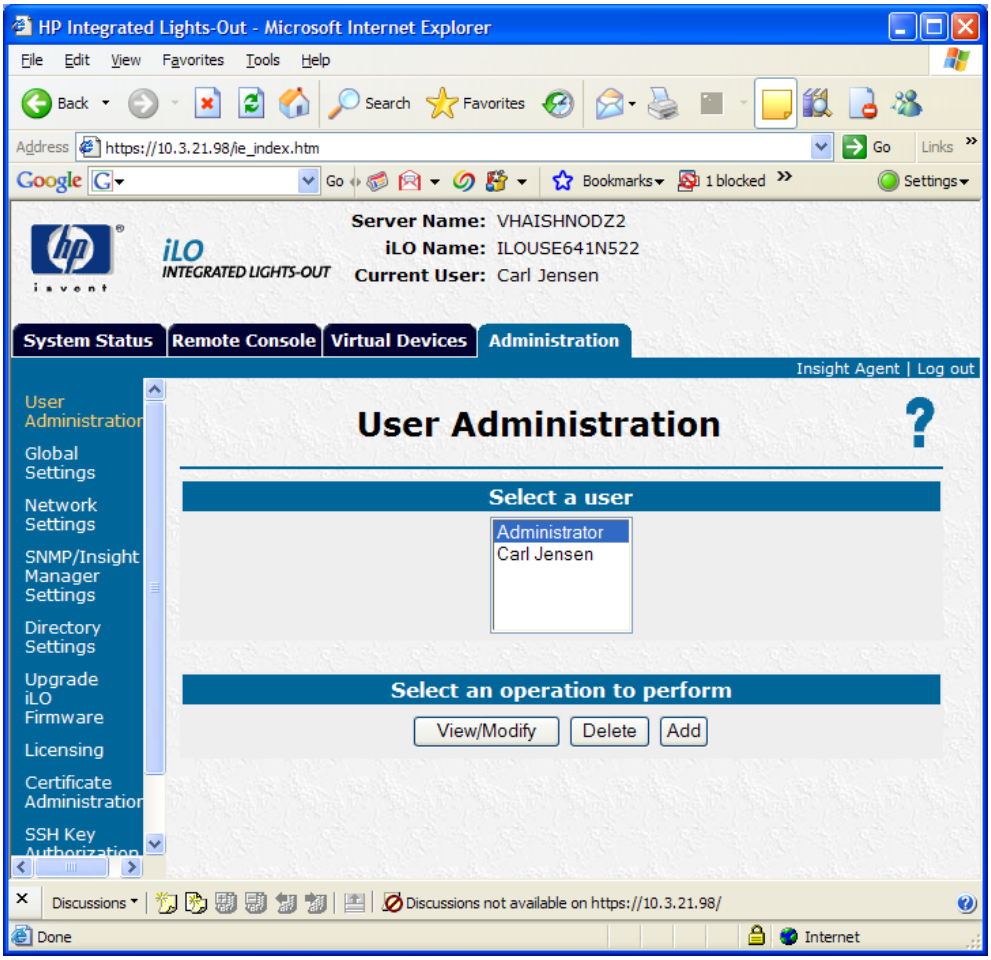
- Virtual Power: Turn the server on or off
- Power Regulator: Adjust power settings
- Virtual Media: Connect to a drive on a remote machine
- Virtual Indicator: Control Server Unit ID light
- Virtual Serial Port: Virtual serial port status
- Virtual Serial Port Configuration: self explanatory

**Figure 39: Virtual Devices tab**

### Administration tab

The **User Administration** item is used to configure iLO users (Figure 40). The other options are not being used at this time.

**Figure 40: Administration tab**



# Maintenance Operations

These maintenance operations are performed, using the VBECS Administrator software, during the initial installation of VBECS and during post-installation maintenance activities.

When VBECS Administrator is used for the first time, Configure Interfaces is the only option available. Completion of Configure Interfaces enables Configure Divisions. Completion of Configure Divisions enables Configure Users.

Configured options will be available at startup to perform maintenance operations.

*Do not change the system! The U.S. Food and Drug Administration classifies this software as a medical device. Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulations. Adding to or updating VBECS software without permission is prohibited.*

- VistALink is installed and running on the associated VistA system.
- The user is defined in VistA, and has a DUZ and Access and Verify Codes necessary to establish a VistA connection.
- The user has a valid Windows account and is defined as a member of the Active Directory (AD) domain group (see Add and Maintain Users in Active Directory).
- The user is defined as a member of the Windows Administrator group on the Active Directory domain group.
- The VBECS database is installed and operational.
- The VBECS BUNDLE 1.0 KIDS build is installed and configured in VistA.
- The VistA data conversion patch LR*5.2*335 is installed in VistA.
- The VistA data conversion is complete.

### Outcome

- Parameters necessary to establish the connection to VistA through VistALink are available to the main VBECS application, as defined in the Configure Interfaces option.
- VBECS-VistA HL7 interface parameters are defined in the Configure Interfaces option.
- One or more divisions are defined for use in VBECS in the Configure Divisions option.
- One or more divisions are activated as local facilities in VBECS in the Configure Divisions option.
- The System Administrator has VBECS login[1] access to all active divisions.
- VBECS users are defined and able to use VBECS in the Configure Users option.

[1] There is a slight difference in terminology between VistA and VBECS: VistA uses “log on” and “logon,” and VBECS uses “log in” and “login.” Therefore, both terms are used throughout this manual. “Log in” and “login” are used generically when referring to both systems at one time.

### Limitations and Restrictions

*When the division changes from full service to transfusion only or from transfusion only to full service, information must be in a final state.*

- The VBECS Administrator performing the initial installation and setup must have the XOBV VISTALINK TESTER option defined as a secondary option in VistA.

### Additional Information

- Refer to the completed Appendix B: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide* for required information when performing maintenance operations.

### User Roles with Access to This Application

VBECS Administrator

### Log Into VBECS Administrator

| User Action | VBECS Administrator |
|---|---|
| 1. To log into VBECS Administrator, double click  (the **Remote Desktop Connection icon**).<br><br>Enter your password. | Displays the user and server names. |
| 2. Double click the **VBECS Administrator icon**. | Opens VBECS Administrator.<br><br>**NOTES**<br><br>When the user logs into VBECS Administrator for the first time to set VistALink parameters, the system does not display the VistA Logon – Authorization screen. Continue at Step 6. |
| 3. Continue to the VistA logon screen (Figure 41). | Opens the VistA Logon – Authorization screen. The user may log onto VistA or continue and log on as needed.<br><br>**NOTES**<br><br>The VistA logon screen is displayed only after initial setup of VistALink parameters. |
| 4. Log onto VistA when VBECS Administrator starts up or at the invocation of any option that uses VistALink when VistALink is not connected. | Allows a user to log on by entering VistA Access and Verify Codes, separated by a semicolon (;), in the Access Code data entry field.<br>When a user accesses an option that requires a VistALink connection and the connection becomes unavailable, allows the user to restore the connection.<br>When a reconnection attempt is successful, VBECS closes the connection status window and returns to the desktop. The VistALink Connected icon in the status bar indicates a successful connection. When a reconnection attempt is unsuccessful, attempts to reconnect to VistALink until the user cancels.<br><br>**NOTES**<br><br>When a user logs into VBECS Administrator, the connection to |

| User Action | VBECS Administrator |
|---|---|
| | VistA is established through VistALink.<br><br>When the VistALink connection is not restorable, VBECS Administrator displays a message that the requested use cannot be executed because VistALink is unavailable. |
| 5. Enter the VistA Access and Verify Codes. | Verifies that user credentials for the VBECS Administrator and VistA Access and Verify Codes belong to the same user. |
| 6. Continue working in VBECS Administrator (Figure 42). | Displays the main menu. |

**Figure 41: Example of VistA Logon**

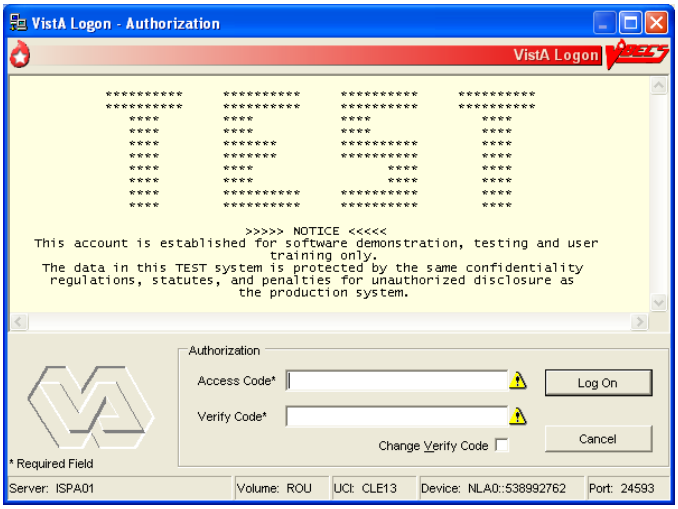
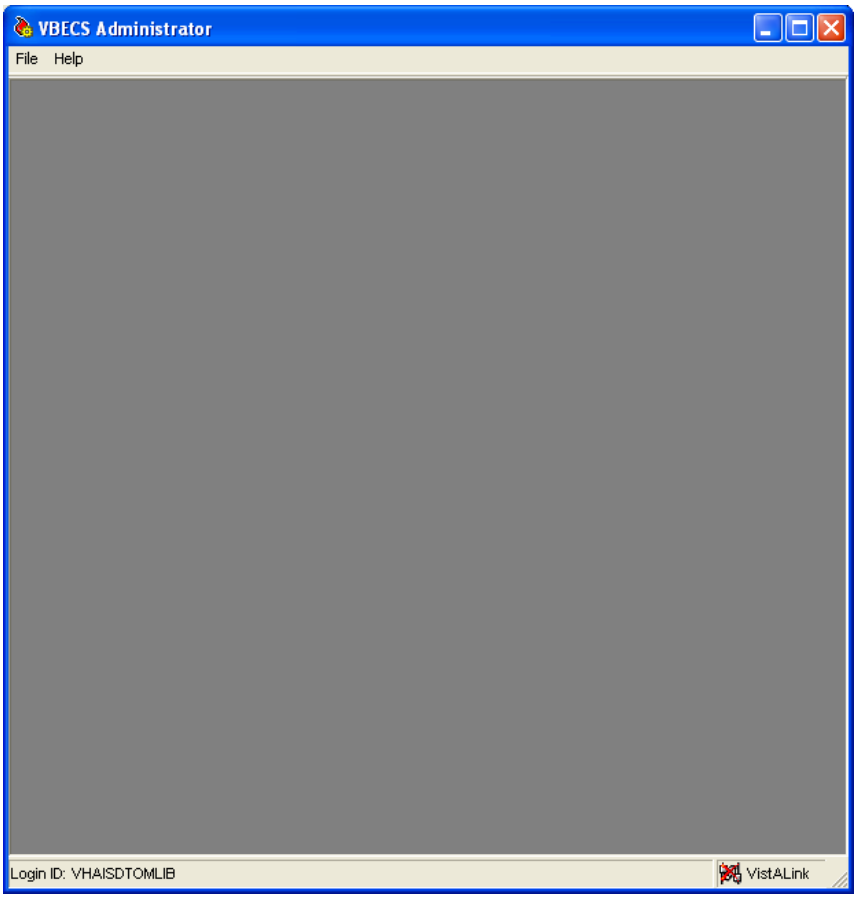


**Figure 42: Example of VBECS Administrator**

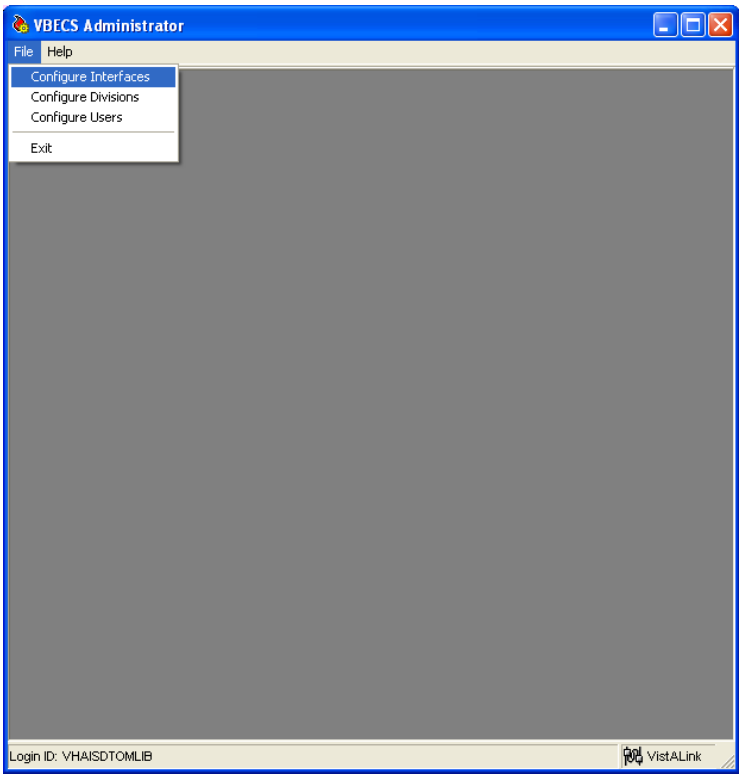


## *Configure Interfaces*

The System Administrator sets parameters for the connection to VistA to enable retrieval of VistA data and to configure HL7 interfaces between VBECS and VistA.

| User Action | VBECS Administrator |
|---|---|
| 1. To configure VBECS VistALink and HL7 interface parameters, click **File** on the main menu of the VBECS Administrator software. | Displays the menu options used to configure VBECS. |
| 2. Click **Configure Interfaces** (Figure 43). | Displays the VBECS Configure Interfaces dialog for data entry. |

**Figure 43: Configure Interfaces**

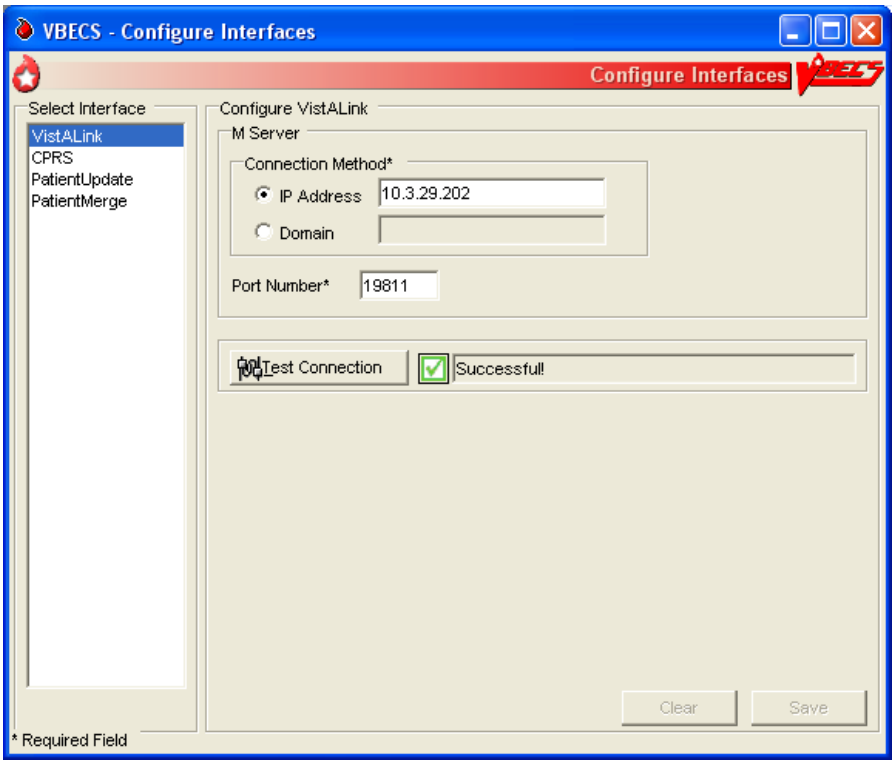



### Configure VistALink Parameters

| User Action | VBECS Administrator |
|---|---|
| 1. To configure VistALink parameters, select **VistALink** from the Select Interface list box (Figure 44). | Displays the Configure VistALink group and allows data entry of the IP address (or domain name) and port number of the VistA system VistALink listener.<br>Allows the user to test the VistALink connection parameters.<br><br>**NOTES**<br><br>The user may modify the IP address (or domain name) and port number, as required. |
| 2. Enter a valid IP address (or domain name) and port number of the VistA system VistALink listener in the M Server group box fields. | Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1) or that the Domain field was filled in.<br>Validates that the port number is a whole number from 1024 to 65535. |

| User Action | VBECS Administrator |
|---|---|
| | **NOTES**<br>The IP Address field represents the VistALink IP address to which VBECS will direct messages. Refer to the Hardware Information section of Appendix B, row 6 for test, and row 7 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.<br><br>The Port Number field represents the VistALink port number to which VBECS will direct messages. Refer to the Hardware Information section of Appendix B, row 8 for test, and row 9 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. |
| 3. Click **Test Connection**.<br><br>Capture a screen shot. | **NOTES**<br>The Test Connection button is enabled only when valid entries exist in the IP Address (or Domain) and Port Number fields.<br><br>If connection to the VistA system is successful, the VistA Logon – Authorization dialog is displayed and the user is required to enter valid Access and Verify Codes.<br><br>If connection to the VistA system is unsuccessful, hover over the red square and a detailed error message will display. |
| 4. Click **Save** to save changes. | Displays a confirmation dialog. |
| 5. Click **Yes** to commit changes to the database. | |

**Figure 44: Configure Interfaces: VistALink**

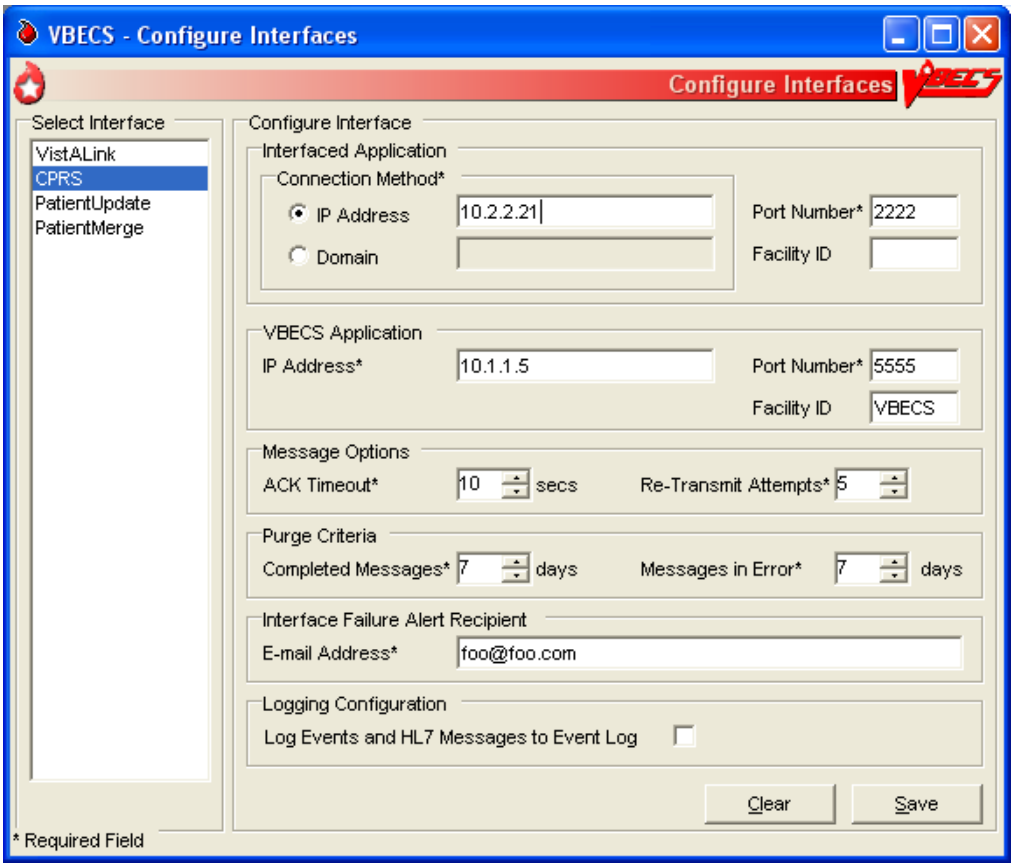


### Configure CPRS HL7 Interface Parameters

| User Action | VBECS Administrator |
|---|---|
| 1. To configure CPRS HL7 Interface Parameters, select **CPRS** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 45). | Displays the Configure Interface group and allows data entry of HL7 interface-related parameters. |
| 2. To configure Interfaced Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields. | Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1) or that the Domain field was filled in.<br>Validates that the port number is a whole number from 1024 to 65535.<br>**NOTES**<br>The IP Address field represents the VistA CPRS IP address to which VBECS will direct messages. The Domain name field represents the fully-qualified domain name to which VBECS will direct messages. Refer to the Hardware Information section of Appendix B, row 6 for test, and row 7 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.<br>The Port Number field represents the VistA CPRS port number to which VBECS will direct messages. Refer to the Hardware Information section of Appendix B, row 10 for test, and row 11 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.<br>The Facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field that is usually set to the primary site's station number. This field is typically validated only when using an interface engine to assist with routing HL7 messages. The VBECS HL7 interfaces do not currently require the use of an interface engine. |
| 3. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields. | Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1).<br>Validates that the port number is a whole number from 1024 to 65535.<br>**NOTES**<br>The IP Address field represents the VBECS cluster server IP address to which CPRS will direct messages. Refer to the Hardware Information section of Appendix B, row 1: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.<br>The Port Number field represents the VBECS cluster server port number to which CPRS will direct messages. Refer to the Hardware Information section of Appendix B, row 4 for test, and row 5 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.<br>The VBECS Facility ID must be different than the VistA. The Facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. This field is validated only when using an interface engine to assist with routing HL7 messages. The |

| User Action | VBECS Administrator |
|---|---|
| | VBECS HL7 interfaces do not require the use of an interface engine.<br><br>The data entered in this group is used by the VBECS CPRS HL7 Listener Service when using a single listener interface. This service is installed as disabled and the VBECS HL7 Multi Listener is enabled. In this configuration, the Port Number field must be set to a port that is not currently used by any other services on the Cluster Server. Refer to the Hardware Information section of Appendix B, rows 4 and 5: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. |
| (This step is optional.)<br><br>4. To configure Message Options group parameters, enter an ACK timeout period and a number of retransmission attempts in the related data fields. | Validates that the ACK timeout period is a whole number from 1 to 999 (seconds) (default: 10).<br>Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5). |
| (This step is optional.)<br><br>5. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields. | Validates that purge periods are whole numbers from 1 to 30 (days) (default: 7). |
| 6. To configure the Interface Failure Alert Recipient group parameter, enter a valid email address in the related data field. | Validates that the interface administrator's email address is entered and conforms to Internet message format RFC 2822.<br><br>**NOTES**<br><br>VBECS Windows Services uses this email address to notify local IRM support or the Blood Bank ADPAC when interface errors occur. |
| 7. To configure the Logging Configuration group parameter, click or clear the **Log Events and HL7 Messages to Event Log** check box.<br><br>Capture a screen shot. | **NOTES**<br><br>This check box indicates whether or not to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Cluster Server. (This is the only way to view VBECS HL7 messages on the VBECS server.) |
| 8. Click **Save** and **Yes** to confirm the save. | |
| 9. To close the VBECS – Configure Interfaces dialog, click in the upper right corner. | Validates that the data was saved. |

**Figure 45: Example of Configure Interfaces: CPRS**

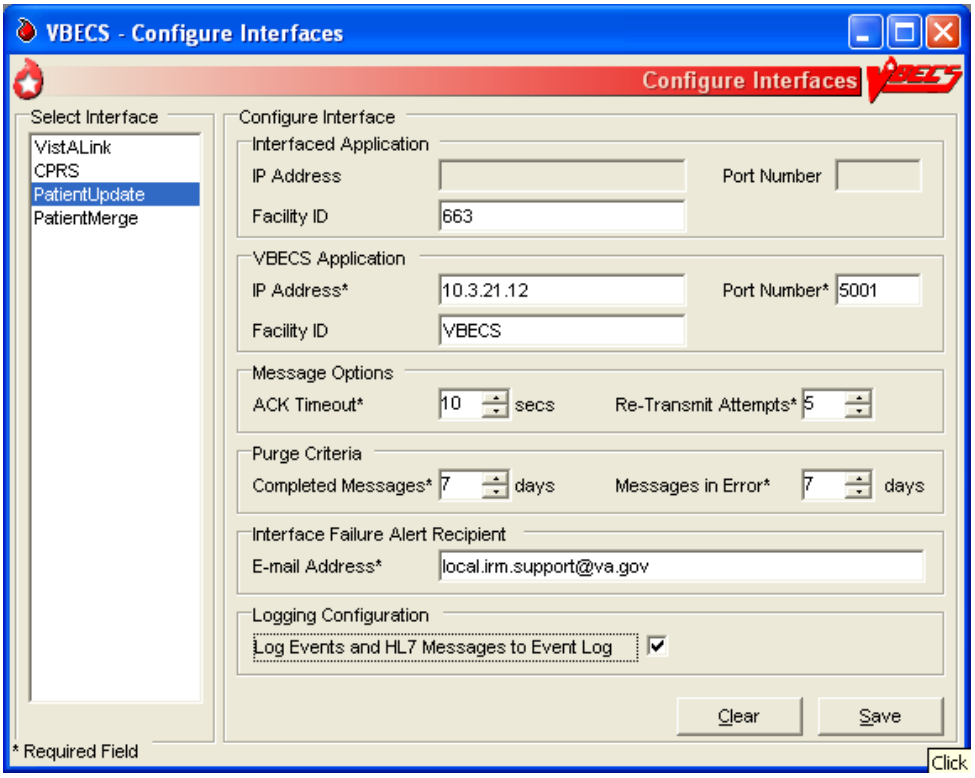


### Configure Patient Update HL7 Interface Parameters

| User Action | VBECS Administrator |
|---|---|
| 1. To configure Patient Update HL7 Interface Parameters, select **PatientUpdate** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 46). | Displays the Configure Interface group and allows data entry of HL7 interface-related parameters. |
| 2. To configure Interfaced Application group parameters, enter a facility ID in the related data fields. | **NOTES**<br>The IP Address and Port Number fields are disabled: no outbound messages are sent to VistA for this interface.<br>The facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. This field is validated only when using an interface engine to assist with routing HL7 messages. The VBECS HL7 interfaces do not require the use of an interface engine. |
| 3. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields. | Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1).<br>Validates that the port number is a whole number from 1024 to 65535.<br>**NOTES**<br>The IP Address field represents the VBECS cluster server IP address to which VistA will direct messages. Refer to the Hardware Information section of Appendix B, row 1: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.<br>The Port Number field represents the VBECS cluster server port number to which VistA will direct messages. Refer to the Hardware Information section of Appendix B, row 4 for test, and row 5 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. |
| (This step is optional.)<br>4. To configure Message Options group parameters, enter an ACK Timeout period and number of retransmission attempts in the related data fields. | Validates that the ACK timeout period is a whole number from 1 to 999 (seconds) (default: 10).<br>Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5). |
| (This step is optional.)<br>5. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields. | Validates that the purge periods are whole numbers from 1 to 30 (days) (default: 7). |
| 6. To configure the Interface Failure Alert Recipient group parameter, enter a valid email address in the related data field. | Validates that the interface administrator's email address is entered and conforms to Internet message format RFC 2822.<br>**NOTES** |

| User Action | VBECS Administrator |
|---|---|
| | VBECS Windows Services uses this email address to notify local IRM support or the Blood Bank ADPAC when interface errors occur. |
| 7. To configure the Logging Configuration group parameter, click or clear **the Log Events and HL7 Messages to Event Log** check box.<br><br>Capture a screen shot. | **NOTES**<br><br>This check box indicates whether or not to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Cluster Server. (This is the only way to view VBECS HL7 messages on the VBECS server.) |
| 8. Click **Save** and **Yes** to confirm the save. | |
| 9. To close the VBECS – Configure Interfaces dialog, click in the upper right corner. | Validates that the data was previously saved. |

**Figure 46: Example of Configure Interfaces: PatientUpdate**

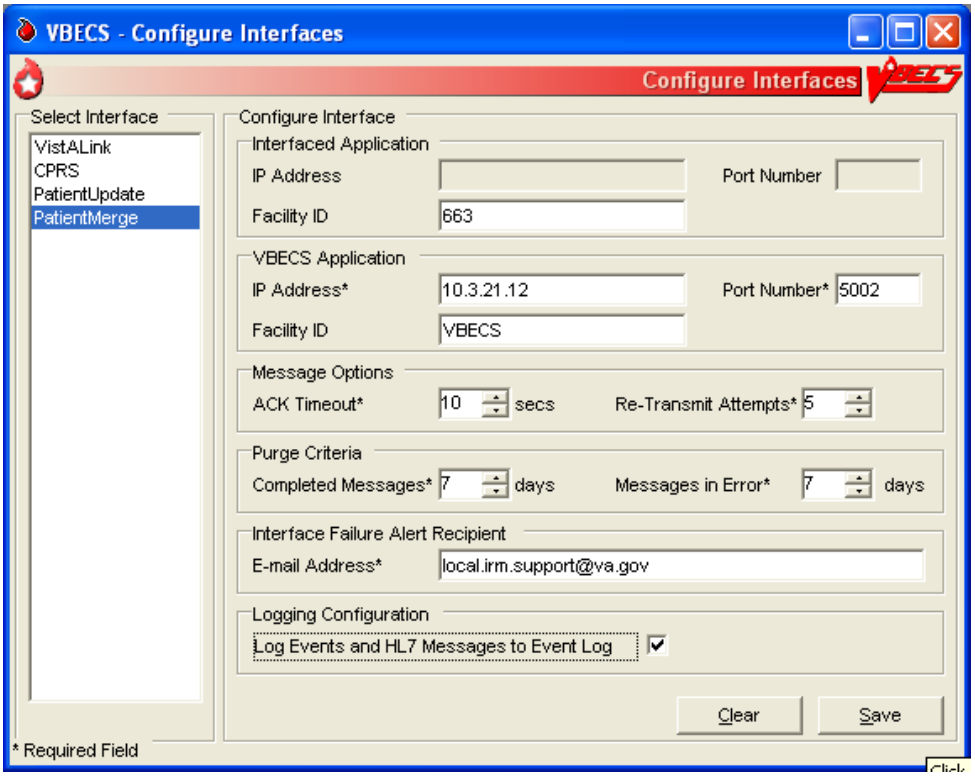


### Configure Patient Merge HL7 Interface Parameters

| User Action | VBECS Administrator |
|---|---|
| 1. To configure Patient Merge HL7 Interface Parameters, select **PatientMerge** from the Select Interface list box in the VBECS – Configure Interfaces dialog (Figure 47). | Displays the Configure Interfaces group and allows data entry of HL7 interface-related parameters. |
| 2. To configure Interfaced Application group parameters, enter a facility ID in the related data field. | **NOTES**<br>The IP Address and Port Number fields are disabled: no outbound messages are sent to VistA for this interface.<br>The facility ID is used in the MSH segment of the HL7 interface to help identify the system. This is a free-text field set to the primary site's station number. This field is validated only when using an interface engine to assist with routing HL7 messages. The VBECS HL7 interfaces do not require the use of an interface engine. |
| 3. To configure VBECS Application group parameters, enter a valid IP address, port number, and facility ID in the related data fields. | Validates that the IP address is in the standard four-octet notation (e.g., 127.0.0.1).<br>Validates that the port number is a whole number from 1024 to 65535.<br>**NOTES**<br>The IP Address field represents the VBECS cluster server IP address to which VistA will direct messages. Refer to the Hardware Information section of Appendix B, row 1: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*.<br>The Port Number field represents the VBECS cluster server port number to which VistA will direct messages. Refer to the Hardware Information section of Appendix B, row 4 for test, and row 5 for production: Configuration Worksheet in *VBECS Application Interfacing Support Software Installation and User Configuration Guide*. |
| (This step is optional.)<br>4. To configure Message Options group parameters, enter an ACK Timeout period and number of retransmission attempts in the related data fields. | Validates that the ACK Timeout period is a whole number from 1 to 999 (seconds) (default: 10).<br>Validates that the number of retransmission attempts for failed messages is a whole number from 1 to 99 (default: 5). |
| (This step is optional.)<br>5. To configure Purge Criteria group parameters, enter the number of days after which completed messages and messages in error are to be purged from the database in the related data fields. | Validates that the purge periods are whole numbers from 1 to 30 (days) (default: 7). |
| 6. To configure the Interface Failure Alert Recipient group parameter, enter a valid email address in the | Validates that the interface administrator's email address is entered and conforms to Internet message format RFC 2822. |

| User Action | VBECS Administrator |
|---|---|
| related data field. | **NOTES**<br>VBECS Windows Services uses this email address to notify local IRM support or the Blood Bank ADPAC when interface errors occur. |
| 7. To configure the Logging Configuration group parameter, click or clear the **Log Events and HL7 Messages to Event Log** check box.<br>Capture a screen shot. | **NOTES**<br>This check box indicates whether or not to record incoming and outgoing HL7 messages in the Application Event Log on the VBECS Cluster Server. (This is the only way to view VBECS HL7 messages on the VBECS server.) |
| 8. Click **Save** and **Yes** to confirm the save. | |
| 9. To close the VBECS – Configure Interfaces dialog, click in the upper right corner. | Validates that the data was previously saved. |

**Figure 47: Example of Configure Interfaces: PatientMerge**




.

## *Configure Divisions*

The System Administrator configures VBECS as a single division or as multidivisional.

### Assumptions

- The VistA data conversion is complete.
- VBECS-VistA connection parameters are set.
- VistALink is installed and running on the associated VistA system.
- The user is defined in VistA, and has a DUZ and Access and Verify Codes necessary to establish a VistA connection.
- The user has a valid Windows account and is defined as a member of the Active Directory domain group (see Add and Maintain Users in Active Directory).
- The IP address of the label printer is known.
- The name of the division report printer is known (if multi-divisional).
- The VBECS database is installed and operational.

### Outcome

- One or more divisions are defined in VBECS.
- One or more divisions are activated as local facilities in VBECS.
- The System Administrator has VBECS login[2] access to all active divisions.

### Limitations and Restrictions

- All units in a division must be in a final status to allow the division to change from full service to transfusion only or from transfusion only to full service.

### Additional Information

- A VBECS Administrator/Supervisor may further configure:
  - VBECS users in Update User Roles.
  - VBECS division parameters in Configure Division, Product Modifications, and Configure Testing.
- The user must log onto VistA using Access and Verify Codes.

### User Roles with Access to This Option

System Administrator

### Add and Maintain Divisions

The user defines and maintains division attributes.

*Changes made in the VBECS Administrator option mapping orders to another VBECS division do not affect delivered orders. Orders delivered to a VBECS division must be completed, rejected, or canceled in that division. Resubmit orders after mapping is completed to send an order to another VBECS division.*

[2] There is a slight difference in terminology between VistA and VBECS: VistA uses "log on" and "logon," and VBECS uses "log in" and "login." Therefore, both terms are used throughout this manual. "Log in" and "login" are used generically when referring to both systems at one time.

| User Action | VBECS Administrator |
|---|---|
| 1. To add and maintain divisions in VBECS, click **File** on the main menu of the VBECS Administrator software. | • Displays the menu options used to configure VBECS. |
| 2. Select **Configure Divisions** (Figure 48). | • Displays the Configure Division dialog and allows entry of division parameters. |
| 3. To edit a defined division, click the **Division Identification** tab (Figure 49). Select a division code or name from the drop-down menu or, to configure a new division, click the **ellipsis** button. Select a division from the list (Figure 50). | **NOTES**<br><br>The user may not edit the division code or name.<br><br>A division may be full service (default) or transfusion only. When a unit not in a final status exists, a user may not change the type of transfusion service.<br><br>When a division is transfusion only, VBECS disables electronic crossmatch.<br><br>When a division changes from full service to transfusion only, units already in inventory are not restricted to patients and must be returned to the blood center.<br><br>When a division changes from transfusion only to full service, inventory units are restricted to patients without ABO/Rh confirmation. The facility must decide how to handle this existing inventory.<br><br>VBECS prevents the user from changing a division from full service to transfusion only or from transfusion only to full service when there are open or partially completed worksheets or processes in the division.<br><br>The Division Name and Division Code are identified in the VistA INSTITUTION file (#4). The Division Name stored in VBECS is the INSTITUTION file NAME field (#.01); the Division Code stored in VBECS is the STATION NUMBER field (#99). When either value change in VistA, rerun these steps to update the VBECS database with the current values from VistA. |

| User Action | VBECS Administrator |
|---|---|
| 4. To receive orders from VistA Institutions to the selected Division, check the Map orders from VistA institutions check box. Click the Active checkbox for each institution that applies. | **NOTES**<br>Changes made to institution mappings require a restart of the VBECS HL7 Multi Listener service. For more information, see Table 6: Windows Service Manager in the VBECS Windows Services section.<br>One or more VistA institutions from the list of valid institutions retrieved from VistA may be associated with the selected VBECS division from the list of valid institutions retrieved from VistA.<br><br>A VistA institution may be associated with only one VBECS division.<br><br>A VistA institution defined as a VBECS division is not eligible for selection as an associated institution to a different VBECS division.<br><br>To associate additional institutions, enable an optional VistALink query to retrieve a list of all institutions associated with the VistA site that are currently defined within the VistA database but not in the selected VBECS division. VBECS displays the list to the user for selection. |
| 5. Select the FDA Registered Facility associated with the division or, to search for the facility by name or FDA Registration Number, click the **ellipsis** button (Figure 49). | • Allows the user to associate a division with a facility from the National Facility Table.<br><br>**NOTES**<br><br>The user must associate a division with a facility from the National Facility Table. If there is no matching facility, VBECS Administrator asks the user to contact the VA Service Desk.<br><br>When this occurs, wait for customer support to respond or, to continue establishing a division, select and configure any facility from the National Facility Table. When the configuration is complete, use the Local Facilities option in VBECS to define the local facility that matches the information missing from the National Facility Table.<br><br>Return to Configure Divisions to re-associate your division with the newly entered local facility.<br><br>When a division is configured, VBECS displays, “I certify that the blood products listed were properly maintained, in accordance with the Code of Federal Regulations, while in storage at this institution. Components were inspected when packed for shipment and found to be satisfactory in color and appearance.” |
| 6. Select the VistA Lab Blood Bank Accession Area associated with the selected division from the drop-down menu (Figure 49). | **NOTES**<br><br>The Lab package uses the Accession Area to track blood bank-related workload for the division. |
| 7. Enter the desired number of minutes in the Lock Inactivity Timeout field. | • Allows the user to set the lock inactivity timeout period (5 to 15 minutes) (default: 5 minutes).<br><br>**NOTES**<br><br>The lock inactivity timeout period specifies how long a user can |

| User Action | VBECS Administrator |
|---|---|
| | be idle and in control of data being edited. VBECS warns the user 60 seconds before the lock inactivity period expires that he will lose priority for the data. When he responds within 60 seconds, VBECS clears the warning and resets the lock activity timer. Otherwise, VBECS informs him that his lock was released and he must reenter his changes.<br><br>VBECS uses optimistic and pessimistic locking to prevent data corruption. If a user attempts to edit data locked by another user, VBECS alerts him that the record is in use and prevents access (pessimistic locking).<br><br>If more than one user attempts to change data simultaneously, VBECS accepts only the first update and warns the other users that the record changed (optimistic locking, which is non-configurable and a fail-safe to pessimistic locking). |
| 8. To activate or inactivate the division, click or clear the **Active VBECS Division?** check box (Figure 49).<br><br>Capture a screen shot. | • When the user saves a previously active division as inactive, inactivates user roles for that division.<br><br>**NOTES**<br><br>The system will not allow the user to activate a division that has orders mapped to another VBECS division. VBECS displays, "Unable to activate. The VBECS division currently has orders mapped to another VBECS division."<br><br>The system will not allow the user to inactivate a division that has orders mapped to it. VBECS displays, "Unable to inactivate. This VBECS division currently has orders mapped to it. Release this mapping prior to inactivation," |
| 9. Click the **Service Type tab**. Click the **Full-Service Facility** or **Transfusion-Only Facility** radio button (Figure 52).<br><br>Capture a screen shot. | • Allows the user to identify the facility as full service or transfusion only.<br><br>**NOTES**<br><br>When the division changes from full service to transfusion only or from transfusion only to full service, information must be in a final state. VBECS does not check for pending orders or active units in inventory, so there is a risk of corrupting information. There is a risk of having unconfirmed units available for transfusion if any are issued. |
| 10. Click the **Printers tab**.<br><br>Clear or click the **Division Uses Label Printer** check box.<br><br>Edit the COM port number and/or the TCP port number.<br><br>Enter the IP address (Figure 53).<br><br>Capture a screen shot. | • Allows the user to enter the COM and TCP port numbers and the IP address for the label printer.<br>• Allows the user to select the default printer for the division when more than one printer is installed on the system.<br>**NOTES**<br><br>Standard values for COM and TCP ports:<br>• COM = 2<br>• TCP = 9100 |
| 11. Click the **Time Zone tab**.<br><br>Select a time zone. | • Allows the user to set the time zone and daylight saving parameters. |

| User Action | VBECS Administrator |
|---|---|
| In the Daylight Savings field, select **US Standard DST**, **Do not observe DST**, or **Custom DST**.<br><br>Enter start and end dates for custom DST (Figure 54).<br><br>Capture a screen shot.<br><br>Click **Save**. | |
| 12. Click **Save** and **OK** to commit the changes or add the new division to the VBECS database. | • Commits changes and additions to the database.<br><br>**NOTES**<br><br>Multidivisional sites must repeat Steps 3–11 for each division.<br><br>The VBECS Administrator/Supervisor who configured the divisions must add himself as a user to all divisions to enable the functionality of canned comments in the VBECS system. |
| 13. To close the **VBECS – Configure Divisions** dialog, click in the upper right corner. | |

**Figure 48: Configure Divisions**

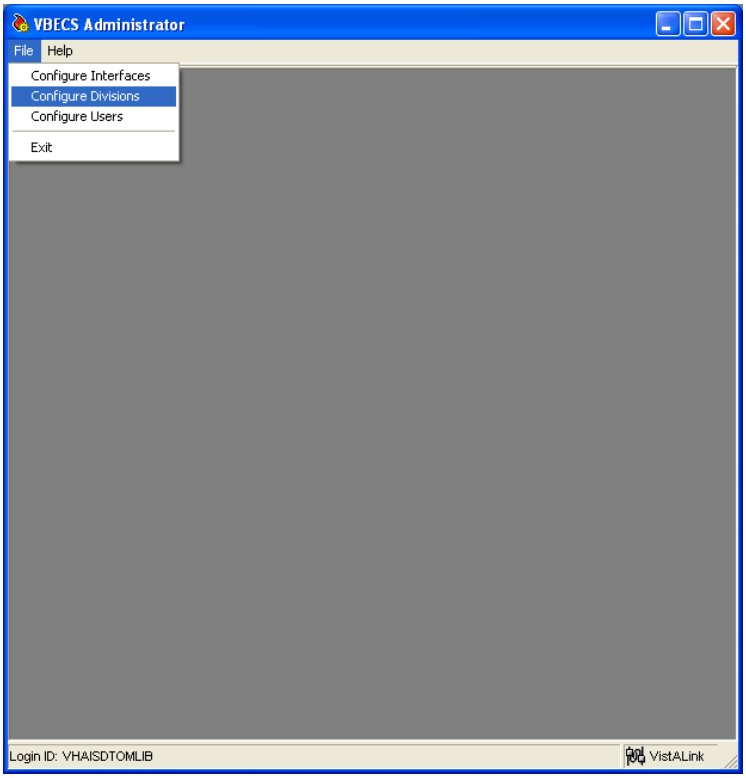


**Figure 49: Example of Configure Division: Division Identification**

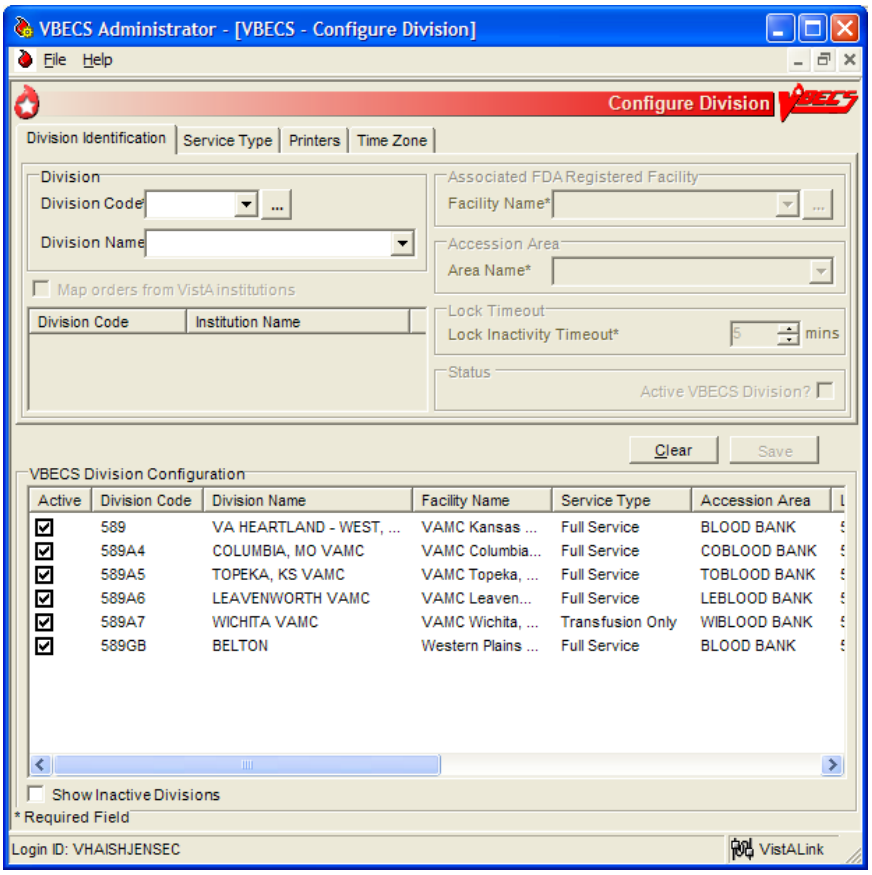



**Figure 50: Example of Select VistA Divisions**

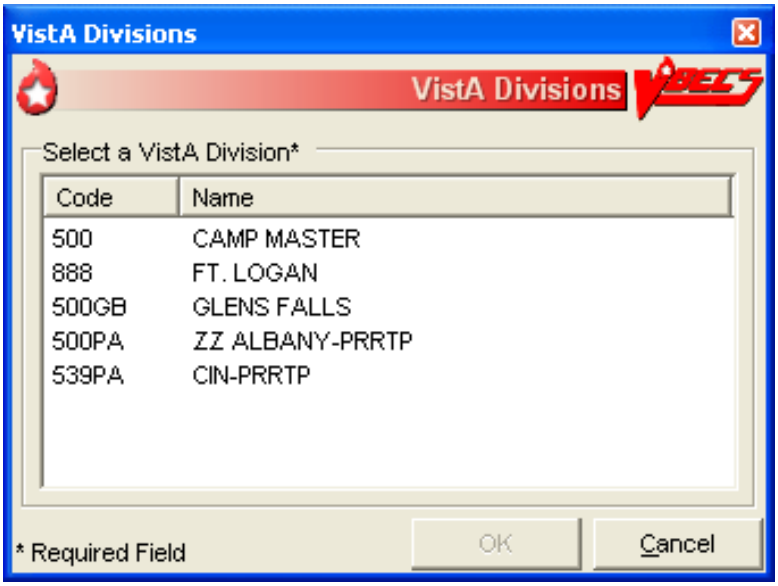


**Figure 51: Example of Facility Search**

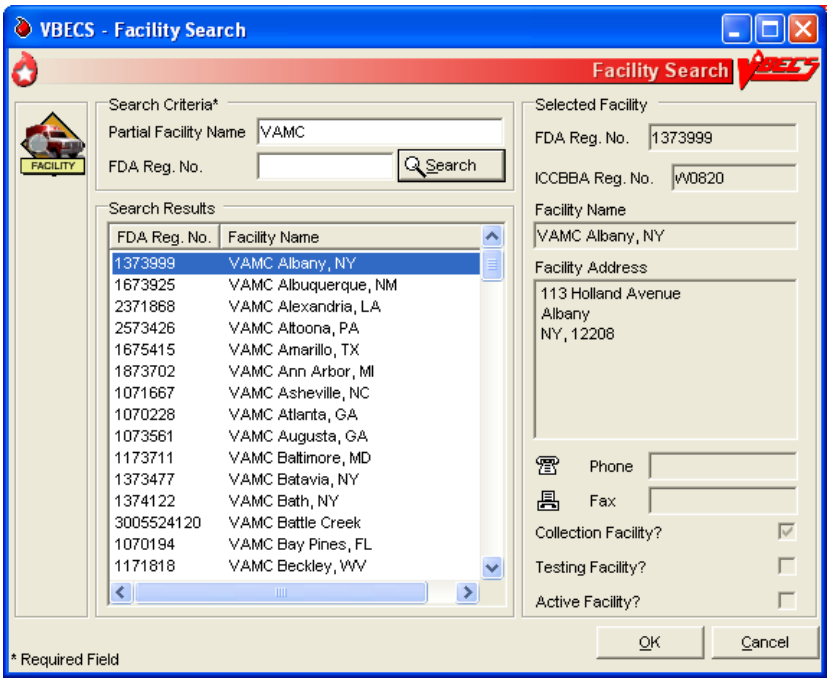



**Figure 52: Example of Configure Division: Service Type**

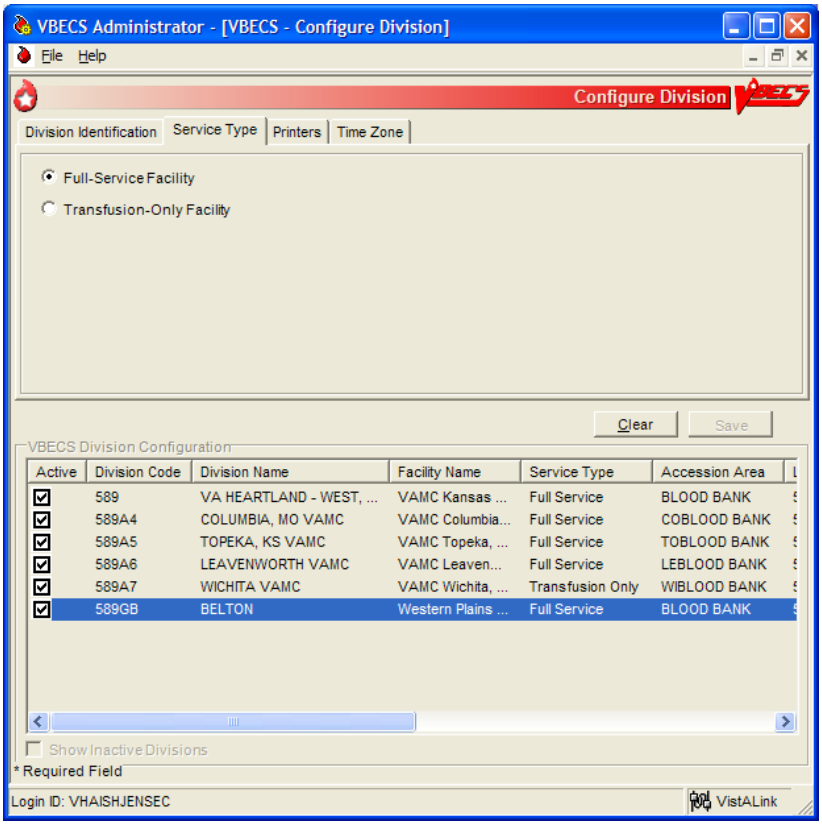


**Figure 53: Example of Configure Division: Label Printing**

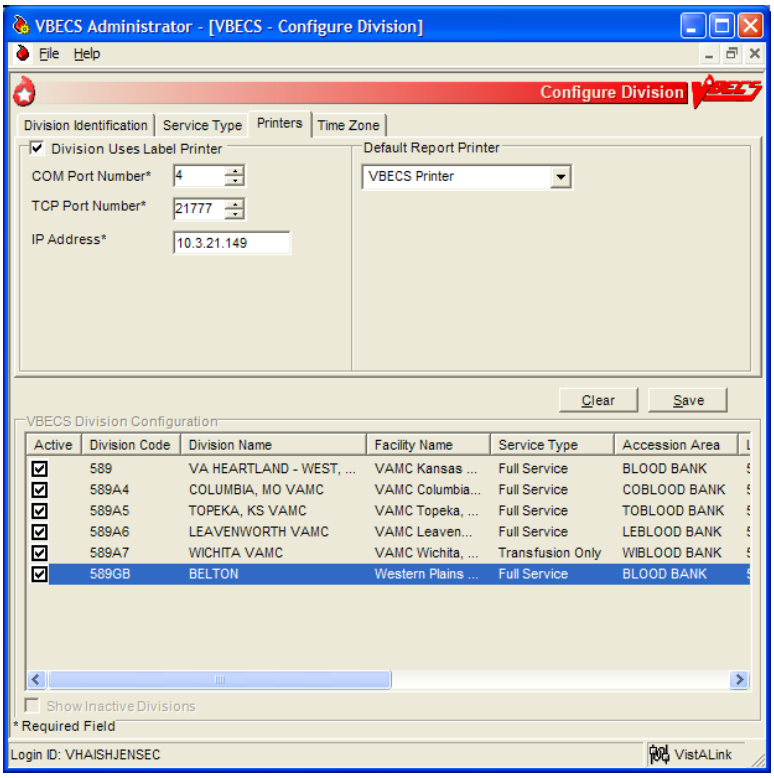
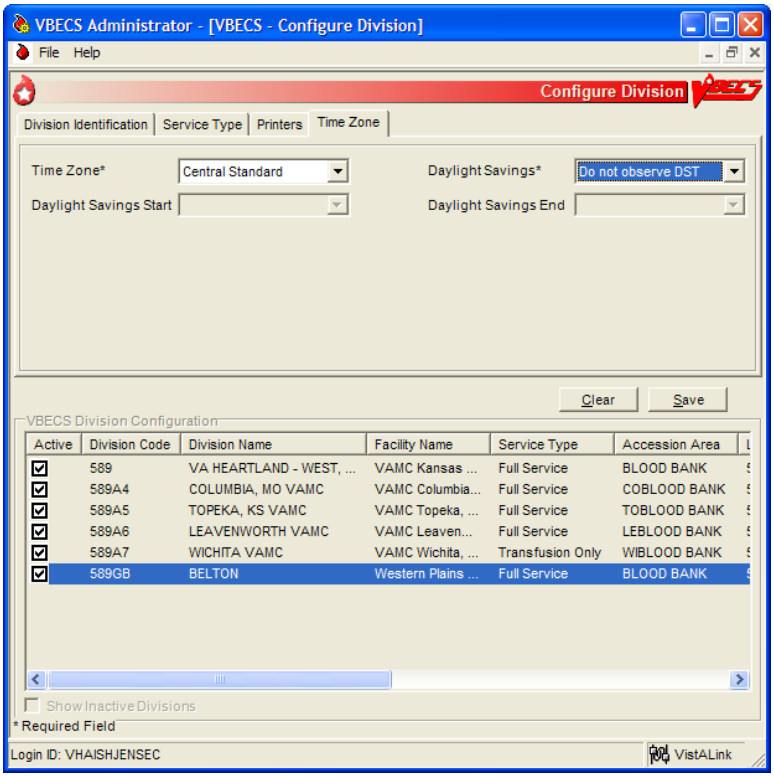



**Figure 54: Example of Configure Division: Time Zone**



## *Configure System Administrators*

Each non-data center site must assign an onsite system administrator to perform regular maintenance tasks such as applying a Windows update and troubleshooting. If your servers reside at a data center, personnel at that location will be administering the servers and you may skip this section.

### Assumptions

- The user has a valid Windows login and was given permission to manage the Active Directory administrator group (set up at installation).
- Users to be configured have a valid Windows account.

### Outcome

- Administrators are defined and able to administer the VBECS servers from the client.

### Limitations and Restrictions

*Each VBECS user must have a unique Windows NT login ID. If a Windows NT login ID becomes inactive and is eligible for re-use in Active Directory, do not re-use it for VBECS: it may result in corrupted data in VBECS.*

### Additional Information

- None

### Add or Remove System Administrators

The user adds and inactivates VBECS users.

| User Action | Active Directory Users and Computers |
|---|---|
| 1. Install Active Directory tools (on the Administrator's computer only) from the Windows Server 2003 Enterprise Edition installation CD or as a free download from Microsoft. | |
| 2. Open the Control Panel.<br><br>Double click **Administrative Tools**.<br><br>Double click **Active Directory Users and Computers** (Figure 55). | • Allows the user to view and add users in Active Directory for VBECS. |
| 3. Navigate to the Organizational Unit (OU) in which your VBECS local groups reside. Double click the name of the user group (on the right) to which you wish to add the user (Figure 56). | • Displays administrator group in the right panel.<br>• Displays the properties window.<br><br>**NOTES**<br><br>• Add a user to the administrator group to allow administrative access to the server through Remote Desktop Connection. |
| 4. Click the **Members** tab (Figure 57).<br><br>Click **Add** to add a user. | **NOTES**<br><br>If the Add button is disabled, you do not have access to this |

| User Action | Active Directory Users and Computers |
|---|---|
| To remove a user, select the user name and click **Remove**. | group. File a Remedy ticket to gain access. |
| 5. If the From this location field does not display the location of the user to be added, click **Locations** and enter the correct domain (Figure 58). | • Allows the user to enter the domain. |
| 6. In the Enter the object names to select field, enter the Windows login ID for the user to be added.<br><br>Click **OK**. | **NOTES**<br><br>Click **Check Names** to verify that the login ID is valid. |
| 7. Click **OK**. | • Closes the Properties window. |
| 8. Exit. | |

**Figure 55: Example of Active Directory Console**

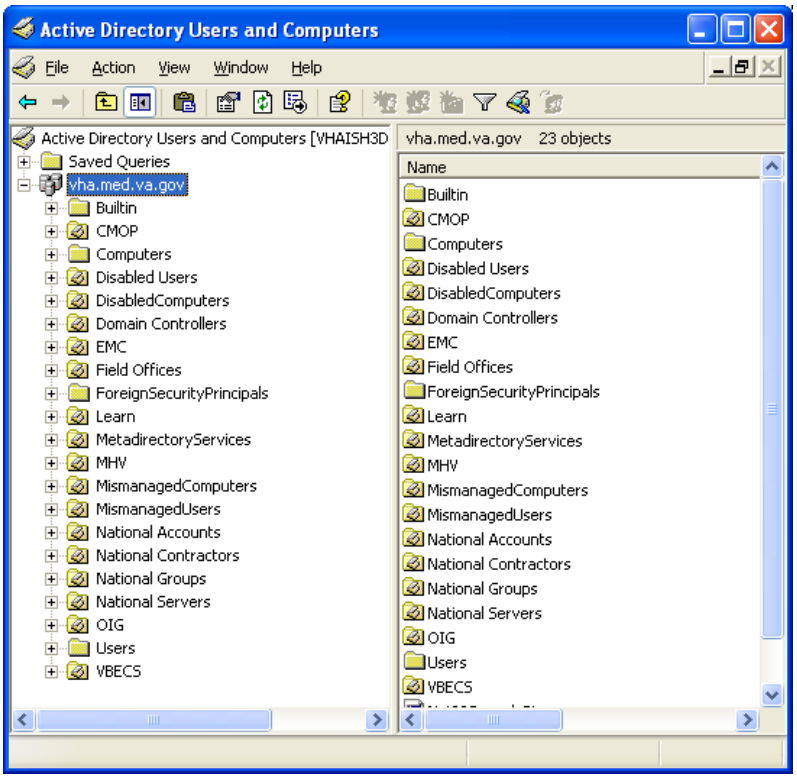


**Figure 56: Example of Administrator User Group**

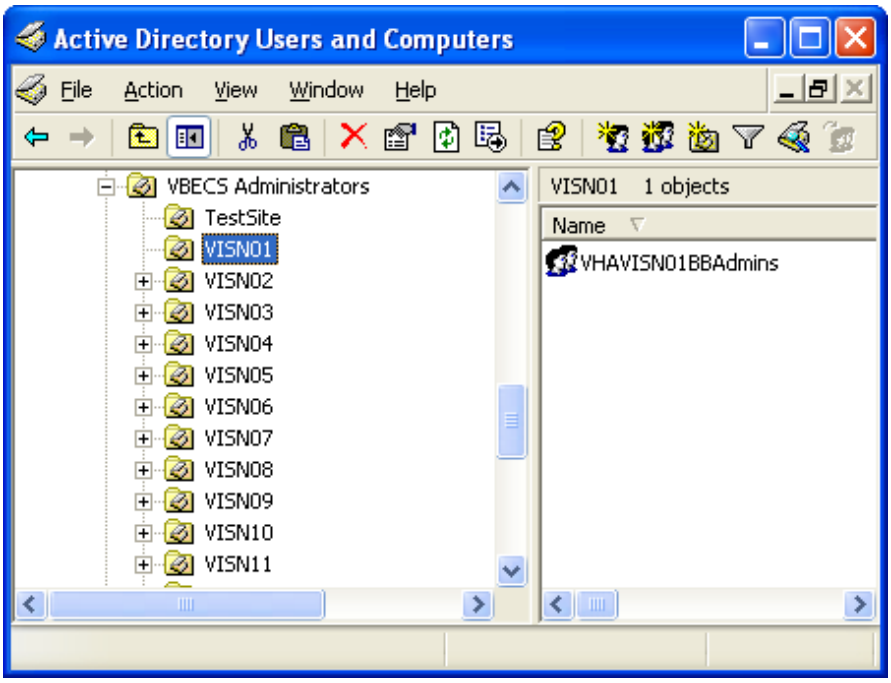



**Figure 57: Example of Group Properties**

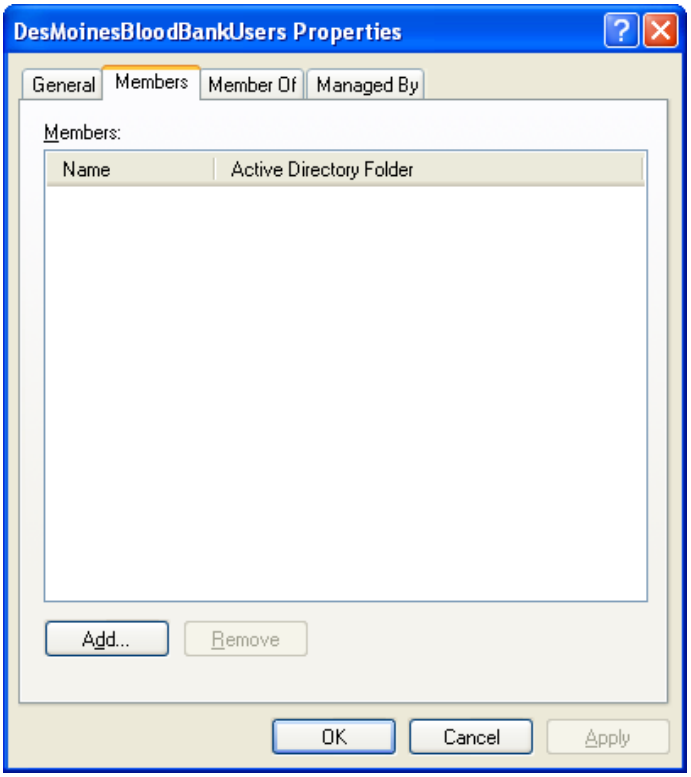
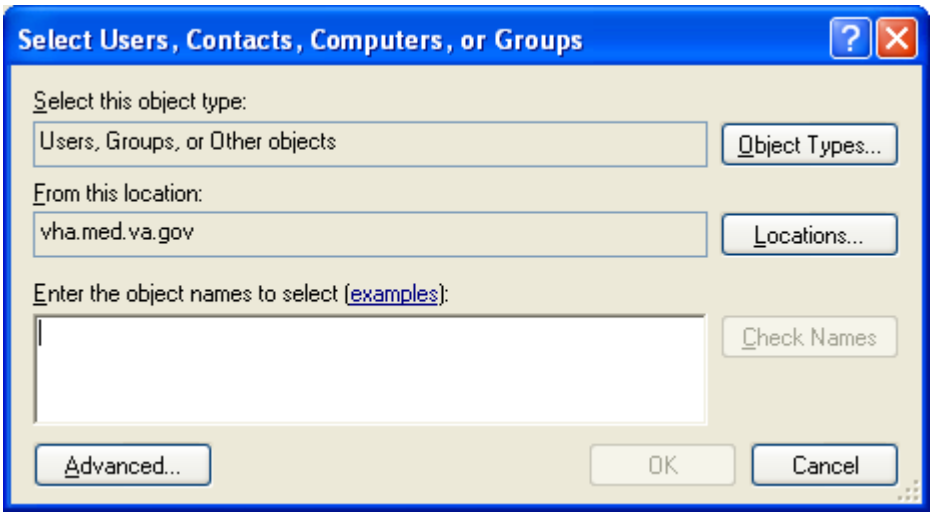


**Figure 58: Example of Select Users**




## *Configure Users*

- The System Administrator matches VistA users to VBECS users and sets user security levels. If this is a data center site, use the form (Appendix D: Active Directory Request Form) to submit Active Directory modifications and skip the "Add and Maintain Users in Active Directory" section (proceed to the "Configure VBECS Users" section after the data center has completed your request).

### Assumptions

- The VistA data conversion is complete.
- VBECS-VistA connection parameters are set.
- VistALink is installed and running on the associated VistA system.
- At least one division in VBECS is configured.
- The user is defined in VistA, and has a DUZ and Access and Verify Codes necessary to establish a VistA connection.
- The user has a valid Windows login and is defined as a member of the Active Directory domain group.
- Users to be configured have a valid Windows account and are defined as members of the Active Directory domain group.
- The System Administrator created Active Directory local groups, as directed in Appendix D: Blood Bank Configuration Checklist, Create Local Groups, in *VistA Blood Establishment Computer Software (VBECS) Installation Guide*.
- The VBECS database is installed and operational.

### Outcome

- VBECS users are defined and able to use VBECS.

### Limitations and Restrictions

*Each VBECS user must have a unique Windows NT login ID. If a Windows NT login ID becomes inactive and is eligible for re-use in Active Directory, do not re-use it for VBECS: it may result in corrupted data in VBECS.*

### Additional Information

- A VBECS Administrator/Supervisor may further configure VBECS users in Update User Roles.
- The user must log onto VistA using Access and Verify Codes.

### User Roles with Access to This Option

System Administrator

### Add and Maintain Users in Active Directory

The user adds and inactivates VBECS users.

| User Action | Active Directory Users and Computers |
|---|---|
| 1. Install Active Directory tools (on the Administrator's computer only) from the Windows Server 2003 Enterprise Edition installation CD or as a free download from Microsoft. | |
| 2. Open the Control Panel.<br><br>Double click **Administrative Tools**.<br><br>Double click **Active Directory Users and Computers** (Figure 59). | • Allows the user to view and add users in Active Directory for VBECS. |
| 3. Navigate to the OU in which your VBECS local groups reside. Double click the name of the user group (on the right) to which you wish to add the user (Figure 60). | • Displays two user groups in the right panel, one for VBECS Administrator and one for VBECS.<br>• Displays the properties window.<br><br>**NOTES**<br><br>The VBECS local groups (V*nnxxx*VbecsUsers and V*nnxxx*VbecsAdministrators, where *nn* is your VISN number and *xxx* is your site identifier) were created in Appendix D: Blood Bank Configuration Checklist, Create Local Groups, in *VistA Blood Establishment Computer Software (VBECS) Installation Guide*.<br><br>The VBECS Administrator/Supervisor who configured the divisions must add himself as a user to all divisions to enable the functionality of canned comments in the VBECS system. He may inactivate himself later without affecting canned comments.<br><br>• Add a user to either group to allow access to the server through Remote Desktop Connection and to VBECS Administrator or VBECS (depending on the group). |
| 4. Click the **Members** tab (Figure 61).<br><br>Click **Add** to add a user.<br><br>To remove a user, select the user name and click **Remove**. | **NOTES**<br><br>If the Add button is disabled, you do not have access to this group. File a Remedy ticket to gain access. |
| 5. If the From this location field does not display the location of the user to be added, click **Locations** and | • Allows the user to enter the domain. |

| User Action | Active Directory Users and Computers |
|---|---|
| enter the correct domain (Figure 62). | |
| 6. In the Enter the object names to select field, enter the Windows login ID for the user to be added.<br><br>Click **OK**. | **NOTES**<br><br>Click **Check Names** to verify that the login ID is valid. |
| 7. Click **OK**. | • Closes the Properties window. |
| 8. Exit. | |

**Figure 59: Example of Active Directory Users and Computers**

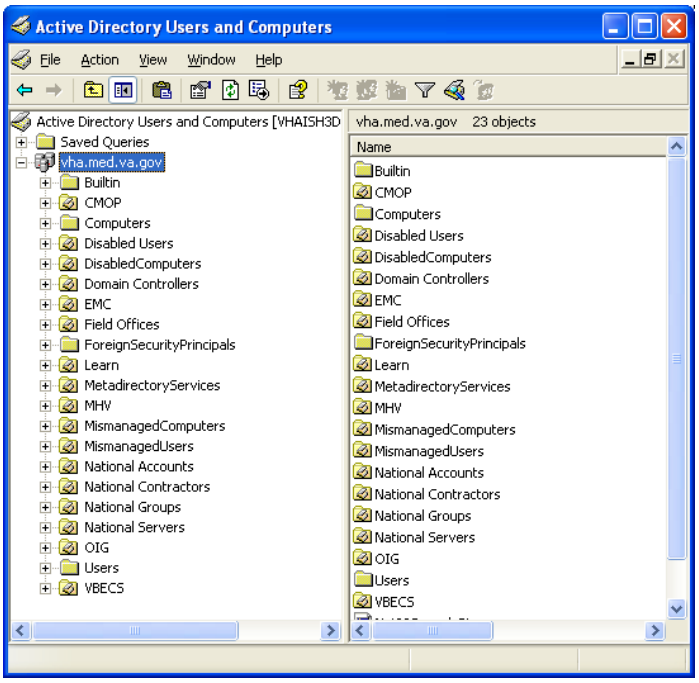


**Figure 60: Example of User Groups**

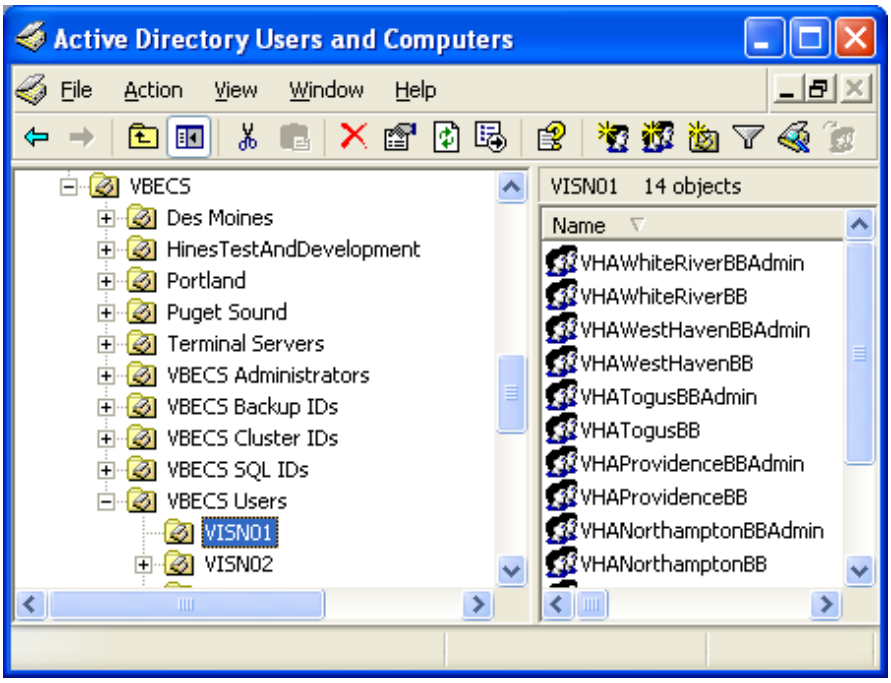



**Figure 61: Example of Group Properties**

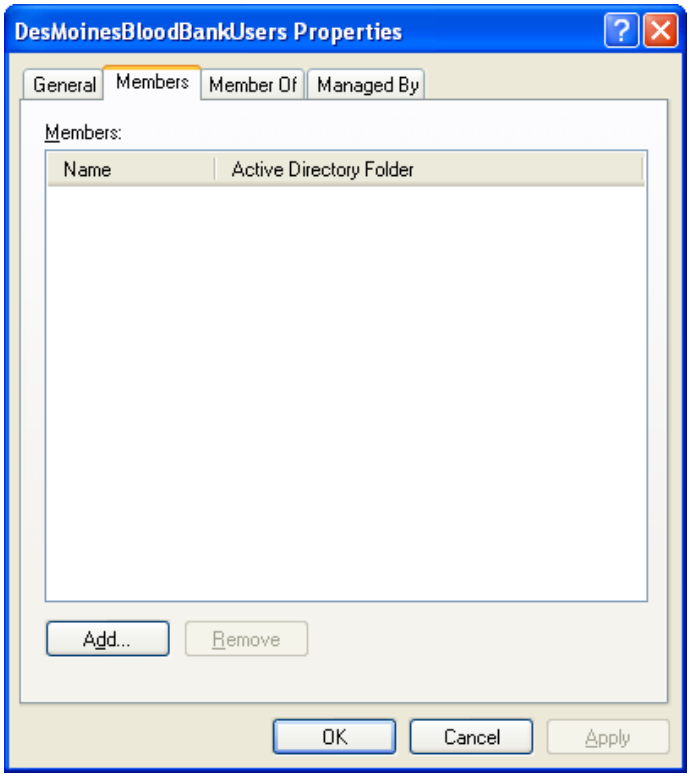
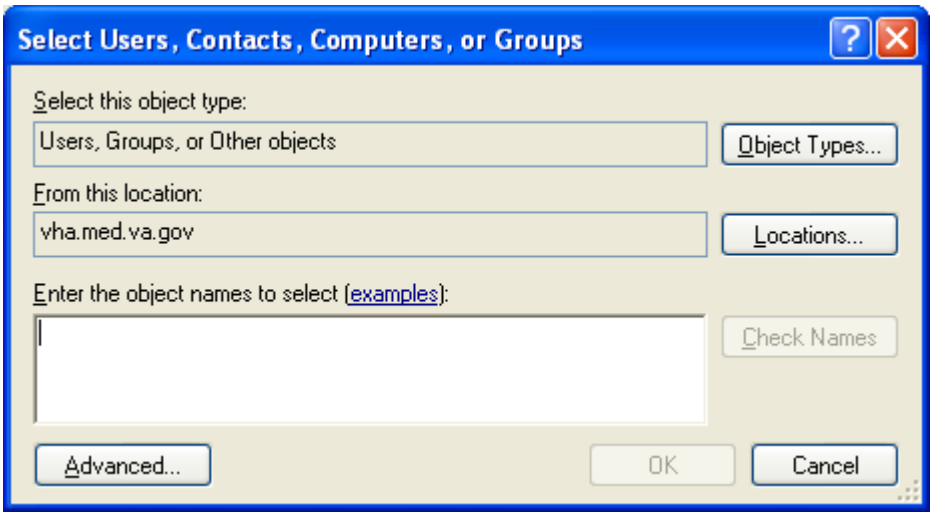


**Figure 62: Example of Select Users**




## Configure VBECS Users

The Active Directory setup must be completed prior to configuring users in VBECS.

| User Action | VBECS Administrator |
|---|---|
| 1. To add and maintain users in VBECS, click **File** on the main menu of the VBECS Administrator software. | • Displays the menu options used to configure VBECS. |
| 2. Select **Configure Users** (Figure 63). | • Allows the user to enter or edit user information. |
| 3. To edit an existing user, select an NT user ID from the drop-down list (Figure 64) or, to search for a new NT user ID to add to VBECS, click the **ellipsis** button to the right of the drop-down list (Figure 65).<br><br>Enter user parameters.<br><br>For each user, VBECS stores:<br>• VistA DUZ<br>• NT Login ID<br>• NT Username<br>• Email Address (optional)<br>• User Initials<br>• Active Status<br>• Division Code<br>• User Role<br>• Division Active Status | • Displays the NT user ID and name.<br><br>**NOTES**<br><br>VistALink lists active VistA Blood Bank users. VistA Blood Bank users are identified by the LRBLOODBANK and LRBLSUPER security keys.<br><br>When VBECS finds users that are inactive in VistA, it asks whether the user wishes to inactivate them in VBECS. **Yes** inactivates the VBECS users. **No** allows the user to continue without inactivating the users (Figure 68).<br><br>The user may not edit the VistA DUZ or user name, the NT login ID or user name, or the division code or name.<br><br>There is a one-to-one correspondence between Windows and VistA users. A VistA DUZ may be associated with only one NT login ID and vice versa.<br><br>The user may:<br>• Activate or inactivate but not delete a defined user from VBECS.<br>• Rescind a defined user's access privileges at one or more divisions but not delete his record or ID from the database.<br><br>The user ID stored in VBECS is the user's NT Logon ID. VBECS displays the data that a user enters in a session. The |

| User Action | VBECS Administrator |
|---|---|
| | user may edit and save the data. When a user cancels, VBECS warns that it will not save the data. VBECS closes the form and returns the user to the main menu screen that may include unrelated open windows.<br><br>VBECS associates the technologist ID, date, time, and division with each process for retrieval by division. |
| 4. To search for a VistA user, click the **ellipsis** button to the right of the VistA DUZ field (Figure 66). | • Allows the user to search for VistA Blood Bank users by name or DUZ.<br><br>**NOTES**<br><br>The user may not edit the VistA DUZ or user name, the NT login ID or user name, or the division code or name. |
| 5. Enter the email address of the user in the E-mail field in the Additional Info group. VistA provides the initials, if available. If not, enter them. | • Allows the user to enter Additional Information about the user for identification.<br><br>**NOTES**<br><br>User initials may be loaded from VistA. VBECS requires unique user initials for use as the technologist ID. |
| 6. To select a VistA division to associate with the user, click the **ellipsis** button to the right of the Division Code drop-down menu (Figure 64). | • Allows the user to select a division to associate with the user<br><br>**NOTES**<br><br>A single user may be associated with multiple divisions. |
| 7. Select a user role from the User Role drop-down menu. Click or clear the **Active Role?** check box to activate or inactivate the role. | • Allows the user to assign security roles to the Blood Bank user.<br>• If a user was removed from the role of Administrator/Supervisor and was the only Administrator/Supervisor user left for a division, displays "You are trying to remove the last Administrator/Supervisor for your division, which would disallow system configuration in the future. You may not proceed." If all entered data is satisfactory, saves user details and access changes to the file and adds or updates the user information in the list view.<br><br>**NOTES**<br><br>One role at a time may be assigned to a user at a division. A user may have only one active user role per division.<br><br>VBECS allows the assignment of a security level to one or more users at a time. VBECS warns that there must be at least one level 6 VBECS Administrator/Supervisor in the division and does not allow the user to change the last Administrator/Supervisor. |
| 8. Click **Update** and **Save**. | • Displays a confirmation dialog. |
| 9. Click **Yes** to commit changes to the database. | • Click **Yes** to commit changes to the database. |
| 10. To close the Edit Users dialog box, click  in the upper right corner. | |

**Figure 63: Configure Users**

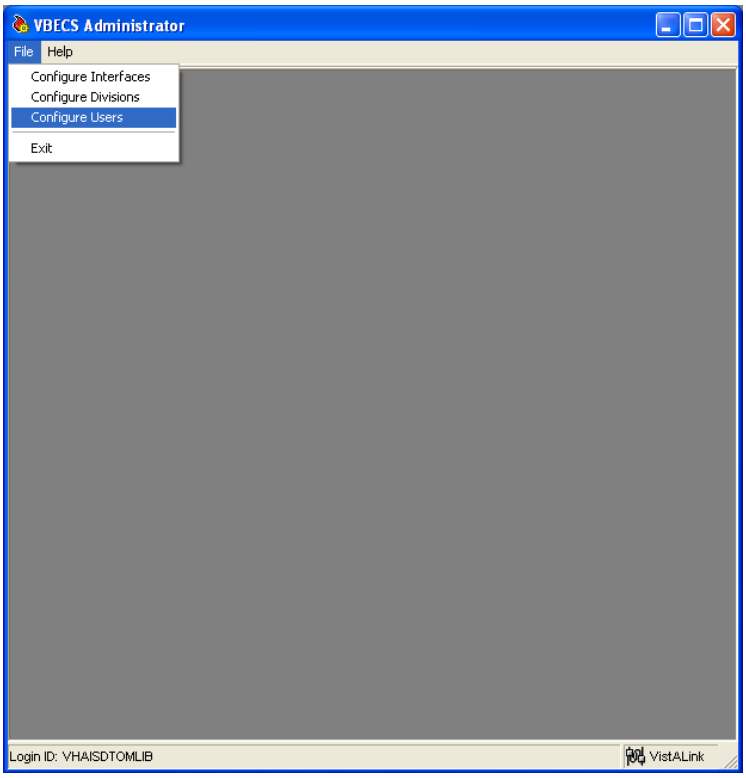



**Figure 64: Example of Edit User**

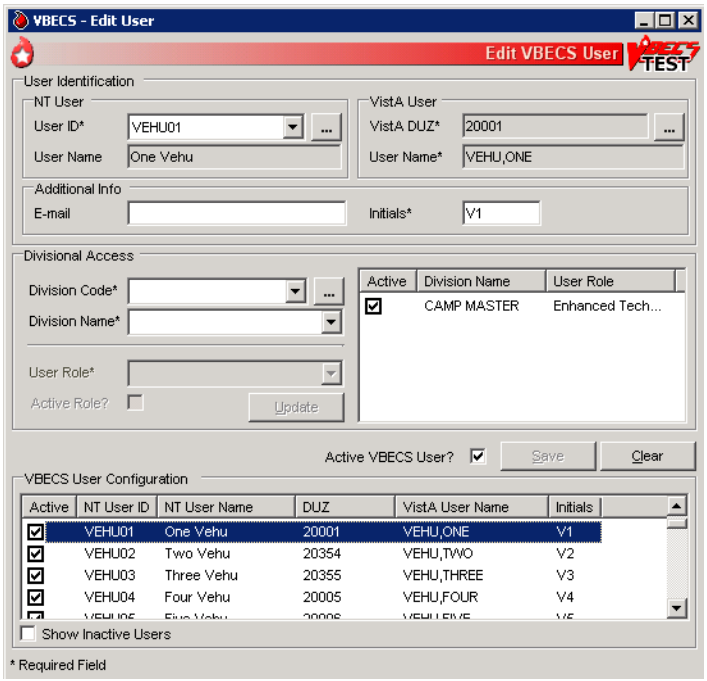


**Figure 65: Example of Windows Users**

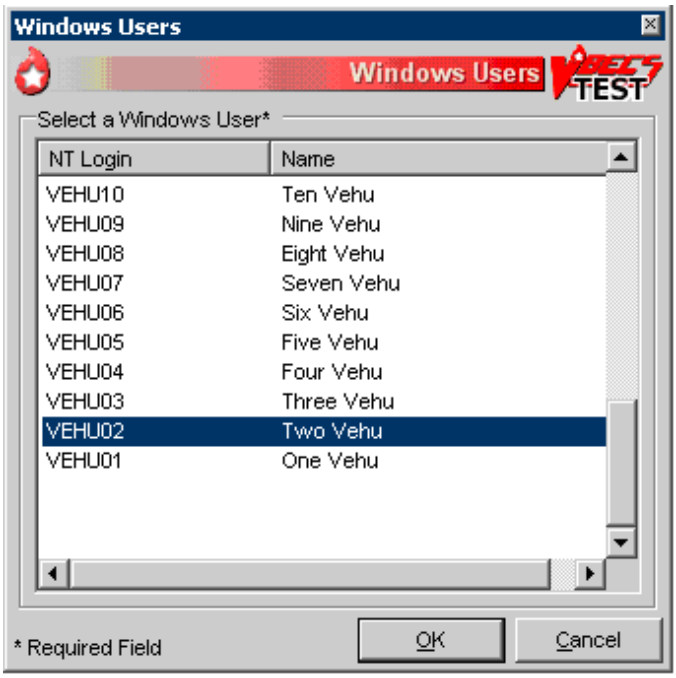



**Figure 66: Example of VistA Users**

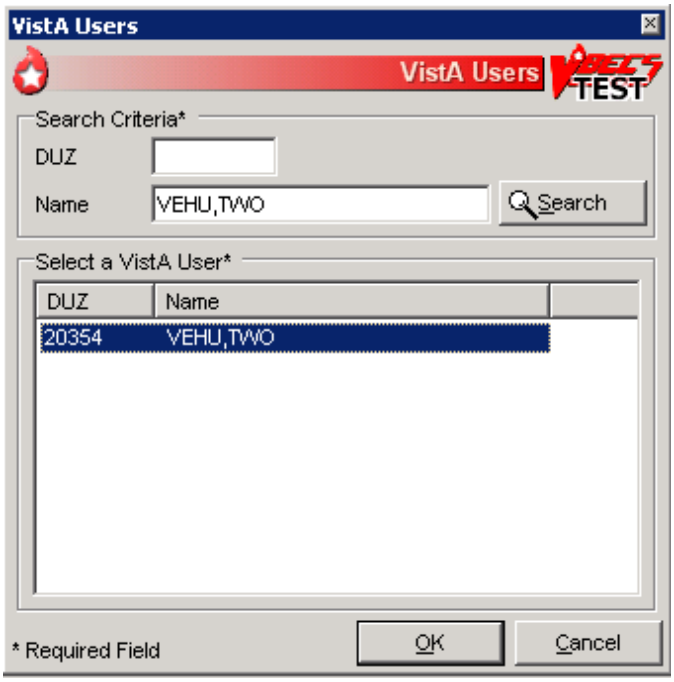


**Figure 67: Example of VistA Divisions**

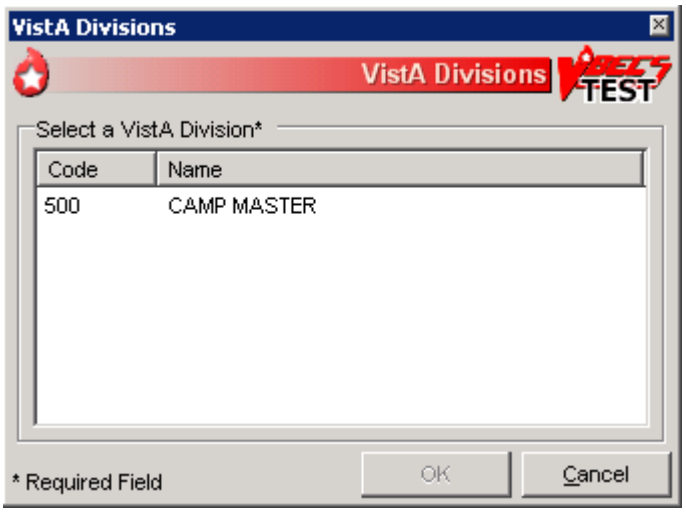
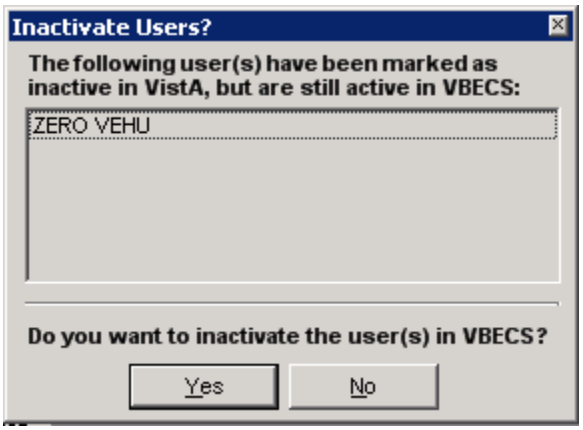



**Figure 68: Example of Inactive Users**



## *Transmit Workload Data*

VBECS workload data is recorded in VBECS when records that qualify as Workload Events are saved in VBECS. This data is transmitted to the VistA Laboratory workload recording system for national and local workload reporting.

### Assumptions

- Workload codes were assigned to VBECS processes using Workload Codes.
- Healthcare Common Procedure Coding System (HCPCS) codes were assigned to blood products using Blood Products.
- A record was saved or inactivated immediately preceding workload data collection.
- The connection to VistA is active.

### Outcome

- Information was transmitted to VistA for inclusion in appropriate reports.

### Limitations and Restrictions

- None

### Additional Information

- Workload Event data must include information required for Decision Support System (DSS), Patient Care Encounter (PCE), and Billing Awareness. Once in VistA, existing VistA functionality will handle required reporting.
- The system accumulates and periodically transmits workload information to the VistA Lab workload recording process. The data is transmitted from VBECS to VistA by the VBECS Workload Capture Remote Procedure called by a nightly Lab background process.

### User Roles with Access to This Option

All users

### Transmit Workload Data

These steps are associated with the "Save" function within any class that performs a Workload Event such as recording a blood test result or interpretation for a unit or a patient, modifying a unit, and pooling units. VBECS must know which classes perform Workload Events and how to classify the work accomplished for reporting. When the database is updated, the VistA technologist ID of the updater, the division, and the date and time of the update are recorded. In some instances, a mechanism to capture Laboratory Management Index Program (LMIP) workload information exists. In addition, for certain events that involve patient processing, the patient location, treating specialty, service, etc., are captured to satisfy PCE or DSS reporting requirements.

These steps address the initial recording of these events.

| User Action | VBECS |
|---|---|
| 1. Click **Save** to save a record from an option. | Creates a Workload Event for every process record saved.<br>Recognizes the activity as a new Workload Event.<br>Checks for required reporting properties based on the type of record being saved.<br>Determines the proper workload codes and other related information to be included.<br><br>**NOTES**<br><br>One or more workload codes can be collected with each Workload Event saved. A workload code may be multiplied for certain Workload Events. |
| 2. Exit. | |

### Inactivate a Workload Event

VBECS updates VistA to inactivate the associated workload information (for a patient or a unit) so that PCE and Billing Awareness can be updated to reflect that the transaction is not valid.

| User Action | VBECS |
|---|---|
| 1. Inactivate a saved record. | Recognizes the activity performed as an inactivation of an existing Workload Event record.<br><br>**NOTES**<br><br>See Appendix B: Workload Process Mapping to Application Option Table. |
| 2. Complete the update and choose to save. | Prompts to confirm the save. Saves workload data.<br><br>**NOTES**<br><br>When a previously saved workload-generating event is invalidated (such as in Remove Final Status, Invalidate Test Results, or invalidating previously logged-in units through Edit Unit Information or Invalidate Shipment), VBECS must create and transmit the same Workload Event information to VistA as a negative number. |
| 3. Confirm the save. | Saves workload data.<br><br>**NOTES**<br><br>When a saved Workload Event is associated with a patient, VBECS needs to link the Workload Event to the patient for future reports. |
| 4. The option ends when the record is saved. | |

## *Notify VBECS Central Administrator*

When maintenance operations are configured, the Implementation Manager notifies the VBECS Central Administrator to install ePolicy and MOM.

This page intentionally left blank.

# External Interfaces

VBECS uses VistALink Remote Procedure Calls (RPCs) and HL7 messaging with Microsoft Windows Services for data exchange using a client-server mode interfacing architecture.

Data exchange between the VBECS medical device software and other VistA applications is maintained by private Database Integration Agreements (DBIAs) with the VBECS Application Interfacing Support Software (VAISS) M software and HL7 messaging specifications with other VistA applications. The VAISS M software in the VistA environment is not classified as a medical device and is, therefore, exempt from the VBECS Blood Bank software FDA 510(k) submission. The purpose of this software is to provide data exchange with other VistA applications through a controlled environment.

When communication failures occur in the VistA environment between VBECS and other VistA applications, MailMan sends an email message to the G.VBECS INTERFACE ADMIN mail group. The message includes details of the error to assist with troubleshooting. Refer to Table 7: Troubleshooting VBECS Application Interfaces in the Troubleshooting section for a list of potential error messages and their solutions.

VBECS is not Clinical Context Management compliant. VBECS utilizes Remote Desktop Connection to connect to its dedicated server. If VBECS were to implement Clinical Context Management, the context would be with the VBECS server environment and require other software such as CPRS to be installed on the VBECS server. This is not compatible with the basic design of the encapsulated medical device.

## *Health Level Seven Interfaces*

The VBECS Health Level Seven (HL7) software is a set of Microsoft .NET libraries written in C sharp (C#) that provide HL7 messaging support for VBECS.

The C# software is invoked by Microsoft Windows Services that run outside the VBECS application on the VBECS Cluster server to allow messaging transactions to occur without user intervention or the need for the VBECS application to be running. Some of the key common functionality provided by the software include:

- Client-Server Transport Layer with HL7 Lower Layer Protocol support
- Message Queuing
- Message parsing and building libraries

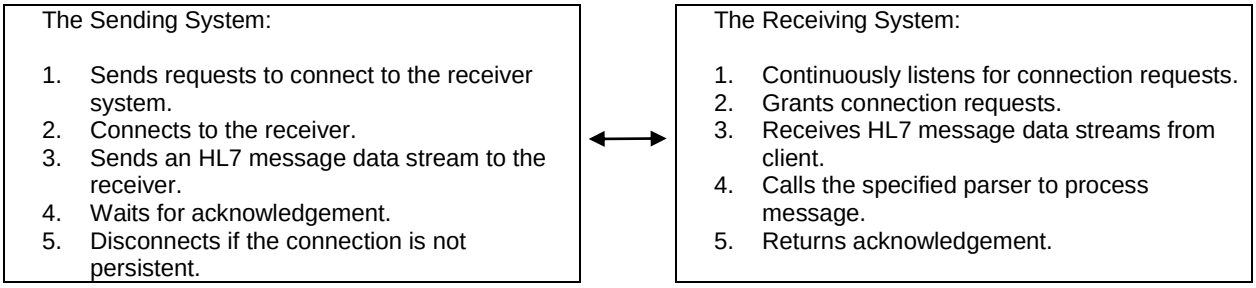
### Client-Server

The C# software provides a transport layer with HL7 Lower Layer Protocol support that uses a client-server architecture to allow bidirectional HL7 message exchange between VBECS and other VistA HL7 enabled applications. The software includes a common communications driver that allows VBECS to send and receive HL7 messages to and from multiple VistA applications. The software was designed to support multiple interfaces running concurrently without the operations of one interface interfering with another.

Each interface requires two separate roles of the client and server.

- Sending System = TCP Client (initiates connection to the Receiving System)
- Receiving System = TCP Server (listens for connections)

**Figure 69: Client-Server Over TCP/IP Channels**




## Transport Layers and Lower Layer Protocols

A transport layer defines the physical connections between VBECS and other systems. Examples include TCP/IP networks and serially cabled connections.

The VBECS HL7 software supports multiple HL7 interfaces developed for VBECS and configured through VBECS Administrator by an authorized user. Some of the information, such as TCP/IP addresses and port numbers, are required by the transport layer and lower layer protocols to provide network connectivity and data exchange with an interfaced system.

An HL7 Lower Layer Protocol (LLP) defines how the systems communicate and exchange HL7 messages across a transport layer. While not defined within the HL7 standard itself, several LLPs are defined in *Health Level Seven Implementation Support Guide*.

LLPs provide the lower layer communication functionalities to exchange messages between systems, such as flow control and error recovery. “Lower layer” refers to a portion of the Open Systems Interconnect (OSI) model, which is divided into seven layers. The lower layers (1 through 4) include the physical connection between the systems and the communications protocol used. The HL7 standard itself defines the seventh and highest application layer.

The VBECS HL7 software supports only the Minimal Lower Layer Protocol (MLLP) over the VA TCP/IP transport layer. More information regarding the MLLP can be found in Section C.4: Minimal Lower Layer Protocol, Appendix B: Lower Layer Protocols, of *Health Level Seven Implementation Support Guide.*

## TCP Client (Sender)

The VBECS HL7 software allows VBECS to send outbound HL7 messages to a TCP/IP listener that supports the MLLP and receive an HL7 acknowledgement message over the same connection. The software provides the transport layer used to deliver the messages and receive the acknowledgement to the message.

To provide guaranteed message delivery of outbound messages from VBECS, all outbound messages will be created when certain events occur and are queued in the VBECS message log. A client monitor service polls the message log periodically to check for new outbound messages and sends them to the receiving system associated with the message type.

## TCP Server (Listener)

All VBECS HL7 Listeners are implemented as Windows Services to provide minimal downtime with minimal user interaction. The default services are configured to start automatically on system reboot by default, but can be changed. HL7 interfaces operate using a single or multi listener Windows Service. The multi listener windows service is the default HL7 listener and can accept and process HL7 messages for all VBECS HL7 interfaces.

## Computerized Patient Record System

Computerized Patient Record System (CPRS) is used to create requests for blood products and diagnostic tests performed in the blood bank with VBECS. An HL7 interface exists between CPRS and VBECS to transmit requests and provide updates regarding the requests to both sides of the interface. VBECS and CPRS exchange data using OMG-O19 General Order Messages and ORG-O20 Response to General Order Message (Acknowledgement) messages.

Orders in VBECS are directed to a VBECS division based on the division associated with the patient location (hospital location) selected in CPRS during the order entry process. If a patient order is associated with a hospital location for a division other than one defined in VBECS, the order will be returned to CPRS and canceled immediately. MailMan will send an email message to the ordering physician in VistA indicating that the order was canceled. The error text associated with the order will indicate that the division is not supported in VBECS. A new order must be created for a hospital location with a valid blood bank division.

## VistA Patient Updates

VBECS maintains a separate patient table for blood bank patients with a limited subset of patient-specific data, provided by the VistA system, for blood bank patient orders created through CPRS. VBECS must maintain updates on patient-specific data when changes are made in the VistA system. The patient-specific data that VBECS maintains includes the patient name, date of birth, date of death, gender, social security number, Integration Control Number (ICN), and the VistA internal entry number from the VistA Patient file. The Registration HL7 interface allows VBECS to receive ADT-A08 HL7 messages for all VistA patient data update events.

## VistA Patient Merges

Occasionally, two entries in the VistA patient file are identified as duplicate records for the same patient and the two records must be merged into one. The duplicate records are validated through existing processes in VistA and are merged into a single record. When this occurs, VBECS must receive notification of the merge event and determine whether either of the two patient records exists in the VBECS Patient table. When matching records are identified, VBECS alerts the user. The user must update the patient record manually to match the VistA record. The MPI Patient Merge HL7 interface allows VBECS to receive ADT-A40 HL7 messages when two VistA patient records are merged into one.

## *VistALink Remote Procedure Calls*

Remote Procedure Calls (RPCs) provide a method of data exchange through VistALink for VBECS. The VBECS software provides data to or receives data from the VAISS located in the VistA M environment through RPCs. This data exchange is controlled through DBIAs between the blood bank medical device software and the VAISS VistA M software.

The VAISS software provides a set of M Application Programmer Interfaces (APIs) that call VBECS RPCs through the VBECS VistALink RPC XML Listener Windows Service and return blood bank data

to other VistA applications. The VAISS software also provides a set of VistA RPCs under the VBECS namespace in the Remote Procedure File (#8994) that are called by the VistA VistALink Listener client-server software. These calls are not public utilities and may be subject to change.

**Table 5: Remote Procedure Calls**

| RPC Name | Database Integration Agreement (DBIA) | This RPC: |
|---|---|---|
| VBECS Order Entry | 4619 | Supports order entry of Blood Bank requests from the Blood Bank order entry dialog in CPRS. |
| VBECS Patient Available Units | 4620 | Provides a list of assigned, crossmatched, autologous and directed blood units that are available for a patient. |
| VBECS Patient Transfusion History | 4621 | Provides a list of past transfusions performed for a patient. |
| VBECS Blood Products | 4622 | Provides a list of orderable blood products, or component classes, to the VistA Surgery package. |
| VBECS Patient Report | 4623 | Provides patient specimen testing results, component requests, and available blood units for a patient to be displayed in CPRS. |
| VBECS Patient ABO_RH | 4624 | Provides the most current ABO Group and Rh Type identified for a patient. |
| VBECS Patient ABID | 4625 | Provides a list of antibodies identified for a patient. |
| VBECS Patient TRRX | 4626 | Provides a list of transfusion reactions for a patient. |
| VBECS Workload Capture | 4627 | Provides Blood Bank workload data to the VistA Laboratory Service package for workload reporting to national and local entities. |
| VBECS Workload Update Event | 4628 | Inserts completed workload-related data into the VBECS database after the VistA Laboratory Services package has completed workload reporting transactions. Upon completion of the insert, the RPC returns an XML response to the VBECS Application Interfacing Support Software that initiated the communication indicating a successful or unsuccessful transaction. |
| VBECS Accession Area Lookup | 4607 | Provides a list of all Laboratory Blood Bank Accession Areas in VistA and their associated divisions to VBECS for workload reporting purposes. |
| VBECS Blood Bank User Lookup | 4608 | Returns a list of all Blood Bank users identified in the VistA system to VBECS. Blood Bank users are identified by the Security Keys of either LRBLOODBANK or LRBLSUPER. |
| VBECS Division Lookup | 4609 | Returns a list of all VAMC divisions associated with a VistA system. |
| VBECS HCPCS Codes Lookup | 4610 | Returns a list of Blood Bank related HCPCS codes to be associated with processes, or procedures, performed in VBECS. |
| VBECS Laboratory Test Lookup | 4611 | Returns a list of VistA Laboratory tests to be associated with blood components in VBECS. |
| VBECS Lab Test Results Lookup | 4612 | Returns a list of VistA Laboratory test results for a patient. |
| VBECS Medication Profile Lookup | 4613 | Returns a list of medications for a patient from the VistA Pharmacy package. |
| VBECS Lab Accession UID Lookup | 4614 | Returns data from the VistA Laboratory Services package based on a Lab order number. The data is used to validate a VBECS specimen test request for a patient and specimen received in the Blood Bank for that test. |
| VBECS Workload Codes Lookup | 4615 | Returns a list of Blood Bank related workload related data that is associated with processes in VBECS. |
| VBECS Patient Lookup | 4616 | Provides a patient lookup function using standard VistA patient lookup criteria. A list of matching patients found in the lookup is |

| RPC Name | Database Integration Agreement (DBIA) | This RPC: |
|---|---|---|
| | | returned to VBECS along with required patient identifiers and demographics. |
| VBECS Provider Lookup | 4617 | Provides a lookup of VistA users that hold the PROVIDER security key. |
| VBECS Hospital Location Lookup | 4618 | Returns a list of hospital locations associated with a division in VistA. |
| VBECS Lab Order Lookup by UID | 4633 | Returns a list of Laboratory Services data related to an order based on a specimen UID. |
| VBECS Dss Extract | 4956 | Provides BloodBank post-transfusion related data to the VistA DSS Blood Bank Extract application for DSS reporting. |

## *VBECS Windows Services*

 *Changes made to individual HL7 listeners must be validated in the test account before using in production.*

 *The VBECS Service Monitor must be stopped before stopping another VBECS service: the VBECS Service Monitor will attempt to restart any VBECS service that was stopped.*

VBECS uses Microsoft Windows Services (services) (Figure 70) to provide minimal downtime and minimal user interaction. The services are installed on each physical server of the VBECS cluster server group. The default services are configured to start automatically with a system reboot. The Multi Listener services (VBECS HL7 Multi Listener and VBECS Test HL7 Multi Listener) are the default listener services. None of the other HL7 listener services are used. The other HL7 listener services exist either for troubleshooting or as a backup. The VBECS HL7 Multi Listener and the individual HL7 listener services cannot be used at the same time. When the VistA HL7 logical links are configured in the Configure Interfaces section of this guide, a single IP address and port is required for each link to send outbound data. For example, the OERR-VBECS link (CPRS) must have an IP address and port number to send the new order information. It cannot send this data to two separate IP addresses and ports. All the single listeners are mutually exclusive and must have unique port numbers. The Install VBECS Services and the VBECS Application section of the VistA Blood Establishment Computer Software (VBECS) Installation Guide describe how these services are installed.

## *Reconfiguring the VBECS HL7 Multi Listener and VistALink Services*

### VBECS HL7 Multi Listener Service (Test)

If changes need to be made to the configuration of the VBECS Test HL7 Multi Listener service due to a change in IP address or port number, first stop the VBECS Service Monitor service, then stop the VBECS Test HL7 Multi Listener service. Navigate to the C:\Program Files\VistA\VBECS Test\WinServices\VBECS Test HL7 Multi Listener, and locate the file named VbecsHL7ListenerService.exe.config.
The file contents will look similar to this example:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>0
    <add key="PrimaryDbConnectionString" value="Connection Timeout=90;Data
Source=VHAISHSQLZ1;Initial Catalog=VBECS_V1_TEST;persist security info=False;packet
size=8192;integrated security=SSPI;Application Name=VBECS" />
    <add key="serviceName" value="VBECS TEST HL7 Multi Listener" />
    <add key="allowPing" value="true" />
    <add key="listenerIpAddress" value="VBECS Cluster IP Address" />
    <add key="listenerPortNumber" value="21993" />
    <add key="monitorService" value="true" />
    <add key="monitorInterval" value="5000" />
    <add key="monitorMaxRetries" value="3" />
    <add key="monitorServiceStartTimeout" value="5" />
```

Change the value for the key named **listenerIpAddress** to the VBECS cluster IP address and the key named **listenerPortNumber** to 21993. Save the file, close it and restart the VBECS Test HL7 Multi Listener service and the VBECS Service Monitor service.

**Note:** All changes must be applied to both the active and passive nodes of the VBECS cluster.

### VBECS HL7 Multi Listener Service (Production)

Edit the production listener (VBECS HL7 Multi Listener) in the same manner as Test. Navigate to C:\Program Files\VistA\VBECS\WinServices\VBECS HL7 Multi Listener, and locate the file named VbecsHL7ListenerService.exe.config.

Change the value for the key named **listenerIpAddress** to the VBECS cluster IP address and the key named **listenerPortNumber** to 21994. Save the file, close it and restart the VBECS HL7 Multi Listener service and the VBECS Service Monitor service.

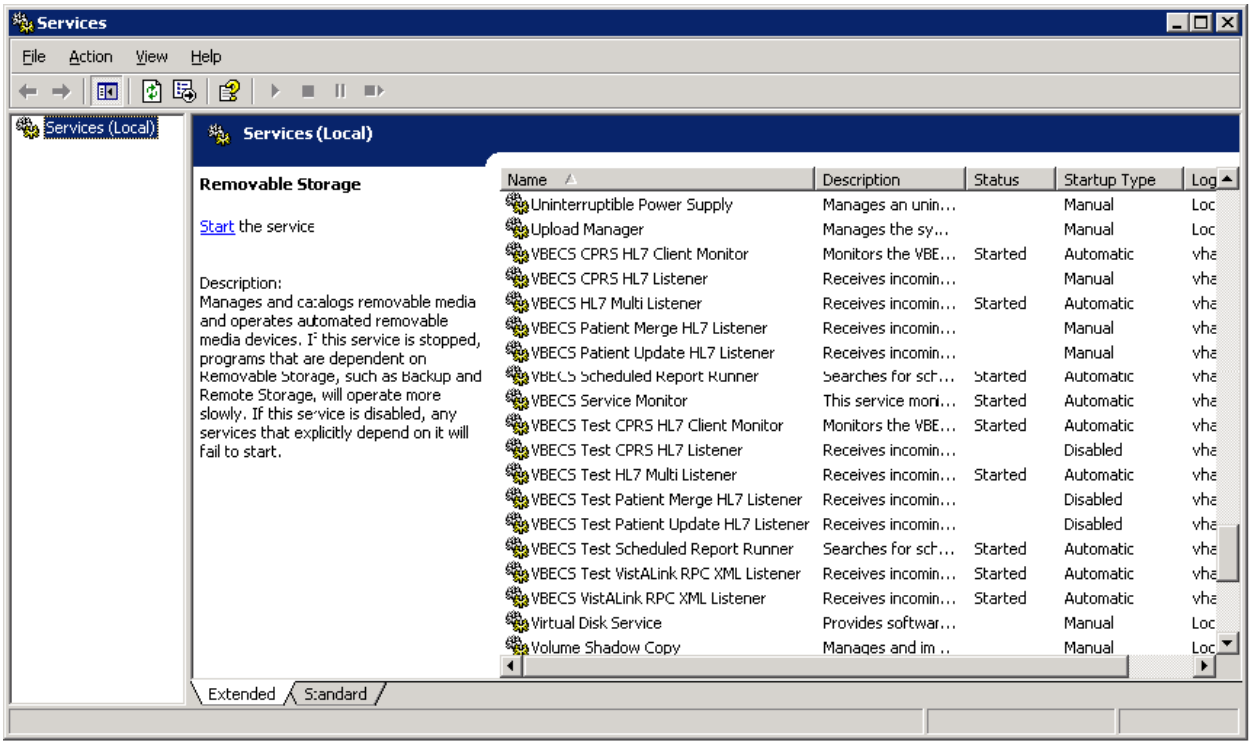
**Note:** All changes must be applied to both the active and passive nodes of the VBECS cluster.

## VBECS Single Listener Service

If troubleshooting requires use of the other listener services, stop the VBECS Service Monitor and VBECS HL7 Multi Listener services. Start the single listeners as required. Once they are configured properly in the Configure Interfaces section of this guide, start the VBECS Service Monitor service.

Use the Windows Service Manager to start, stop, or view the status of a VBECS service. To open the Windows Service Manager, click **Start**, **Control Panel**, **Administrative Tools**, **Services**.

**Figure 70: Example of Services**




## VBECS VistALink Service (Test)

If changes need to be made to the configuration of the VBECS Test VistALink RPC XML Listener service due to a change in IP address or port number, first stop the VBECS Service Monitor service, then stop the VBECS Test VistALink RPC XML Listener service. Navigate to the c:\Program Files\VistA\VBECS Test\WinServices\VBECS Test VistALink RPC XML Listener, and locate the file named VistALink.Listener.WinService.exe.config.

The file contents will look similar to the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <sectionGroup name="VistALink">
      <section name="RpcList"
type="gov.va.med.vbecs.DAL.VistALink.Listener.Core.RpcListConfigSectionHandler,VistALi
nk.Listener.Core" />
    </sectionGroup>
  </configSections>
  <appSettings>
    <add key="PrimaryDbConnectionString" value="Connection Timeout=90;Data
Source=vhaishsqlz1;Initial Catalog=VBECS_V1_TEST;persist security info=False;packet
size=8192;integrated security=SSPI;Application Name=VBECS" />
    <add key="serviceName" value="VBECS Test VistALink RPC XML Listener" />
    <add key="serverName" value="vhaishsqlz1" />
    <add key="databaseName" value="VBECS_V1_TEST" />
    <add key="listenerPortNumber" value="21991" />
    <add key="allowPing" value="true" />
    <add key="listenerIpAddress" value="VBECS Cluster IP Address" />
    <add key="monitorService" value="true" />
    <add key="monitorInterval" value="3000" />
    <add key="monitorMaxRetries" value="3" />
```

Change the value for the key named **listenerIpAddress** to the VBECS cluster IP address and the key named **listenerPortNumber** to 21991. Save the file, close it and restart the VBECS Test VistALink RPC XML Listener service and the VBECS Service Monitor service.

**Note:** All changes must be applied to both the active and passive nodes of the VBECS cluster.

## VBECS VistALink Service (Production)

Edit the production listener (VBECS VistALink RPC XML Listener) in the same manner as Test. Navigate to C:\Program Files\VistA\VBECS\WinServices\VBECS VistALink RPC XML Listener, and locate the file named VistALink.Listener.WinService.exe.config.

Change the value for the key named **listenerIpAddress** to the VBECS cluster IP address and the key named **listenerPortNumber** to 21992. Save the file, close it and restart the VBECS VistALink RPC XML Listener service and the VBECS Service Monitor service.

**Note:** All changes must be applied to both the active and passive nodes of the VBECS cluster..

All VBECS services start with the VBECS namespace prefix. There are duplicate services for production and test accounts that provide functionality for their respective databases.

**Table 6: Windows Service Manager**

| Windows Service Name | This Service: |
|---|---|
| VBECS CPRS HL7 Client Monitor | Is configured to start automatically at system startup. It polls the VBECS Production database for HL7 update messages to be sent to CPRS in the VistA Production account. |
| VBECS CPRS HL7 Listener | Is initially installed as disabled. It is a single listener HL7 service for the Production CPRS HL7 interface. It should be used only as a backup for the VBECS HL7 Multi Listener service or for troubleshooting HL7 interface problems so that other HL7 interfaces using the multi listener are not adversely affected. |
| VBECS HL7 Multi Listener | Is configured to start automatically at system startup. This is the default HL7 listener service for all Production HL7 interfaces. |
| VBECS Patient Merge HL7 Listener | Is installed as disabled initially. It is a single listener HL7 service for the Production Patient Merge HL7 interface. It should be used only as a backup for the VBECS HL7 Multi Listener service or for troubleshooting HL7 interface problems so that other HL7 interfaces using the multi listener are not adversely affected. |
| VBECS Patient Update HL7 Listener | Is installed as disabled initially. It is a single listener HL7 service for the Production Patient Update HL7 interface. It should be used only as a backup for the VBECS HL7 Multi Listener service or for troubleshooting HL7 interface problems so that other HL7 interfaces using the multi listener are not adversely affected. |
| VBECS Scheduled Report Runner | Is configured to start automatically at system startup. It runs scheduled VBECS reports for the Production database. |
| VBECS VistALink RPC XML Listener | Is configured to start automatically at system startup. It provides a client-server TCP/IP listener service for VistALink RPC XML messages from the VAISS APIs. It calls VBECS RPCs to provide Blood Bank data from the VBECS Production database to VistA Production account applications. |
| VBECS Test CPRS HL7 Client Monitor | Is configured to start automatically at system startup. It polls the VBECS Test database for HL7 update messages to be sent to CPRS in the VistA Test account. |
| VBECS Test CPRS HL7 Listener | Is installed as disabled initially. It is a single listener HL7 service for the Test CPRS HL7 interface. It should be used only as a backup for the VBECS Test HL7 Multi Listener service or for troubleshooting HL7 interface problems so that other HL7 interfaces using the multi listener are not adversely affected. |
| VBECS Test HL7 Multi Listener | Is configured to start automatically at system startup. This is the default HL7 listener service for all Test HL7 interfaces. |
| VBECS Test Patient Merge HL7 Listener | Is installed as disabled initially. It is a single listener HL7 service for the Test Patient Merge HL7 interface. It should be used only as a backup for the VBECS Test HL7 Multi Listener service or for troubleshooting HL7 interface problems so that other HL7 interfaces using the multi listener are not adversely affected. |
| VBECS Test Patient Update HL7 Listener | Is installed as disabled initially. It is a single listener HL7 service for the Test Patient Update HL7 interface. It should be used only as a backup for the VBECS Test HL7 Multi Listener service or for troubleshooting HL7 interface problems so that other HL7 interfaces using the multi listener are not adversely affected. |
| VBECS Test Scheduled Report Runner | Is configured to start automatically at system startup. It runs scheduled VBECS reports for the Test database. |
| VBECS Test VistALink RPC XML Listener | Is configured to start automatically at system startup. It provides a client-server TCP/IP listener service for VistALink RPC XML messages from the VAISS APIs. It calls VBECS RPCs to provide Blood Bank data from the VBECS Test database to VistA Test |

| Windows Service Name | This Service: |
|---|---|
| | account applications. |
| VBECS Service Monitor | Is configured to start manually at system startup. It monitors all VBECS Production and Test services to ensure that they are running and accepting incoming requests, where appropriate. It should be started manually when the VBECS server is rebooted to allow the other services to start first. |

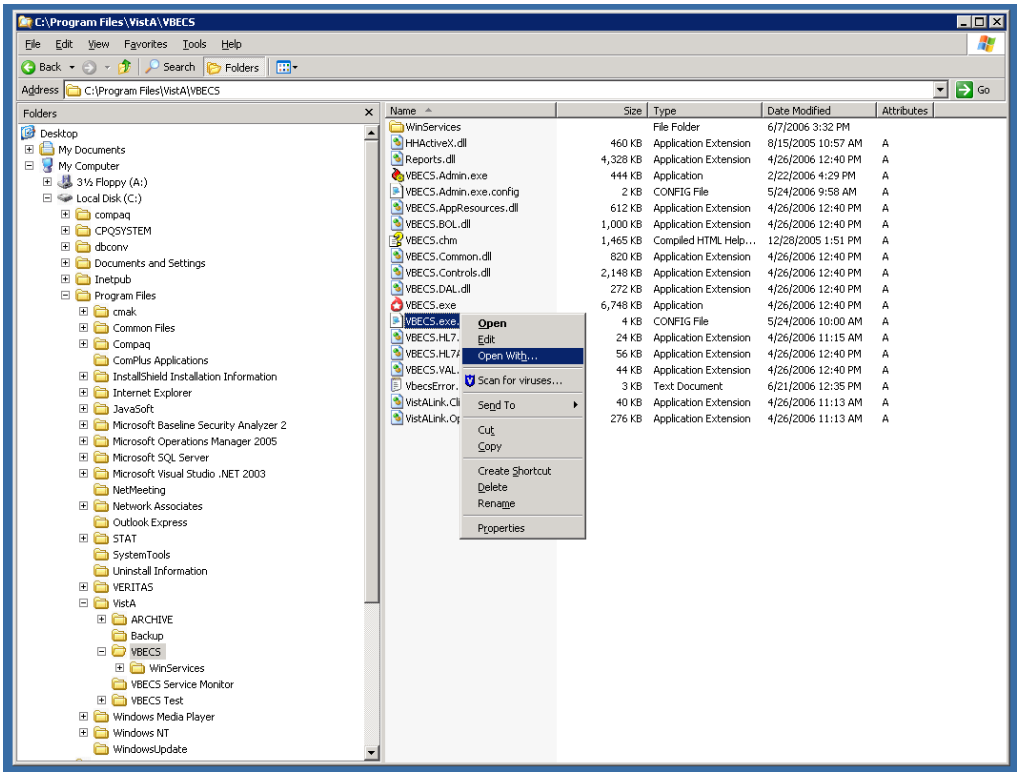
# Troubleshooting

## VistA Query Timeout

The VistA cache refresh interval is the time (in seconds) that VBECS waits before it attempts to copy new VistA data to the VBECS database (to cache it). VistA data is cached for Workload Codes, CPT Codes, HCPCS Codes, and Hospital Locations.

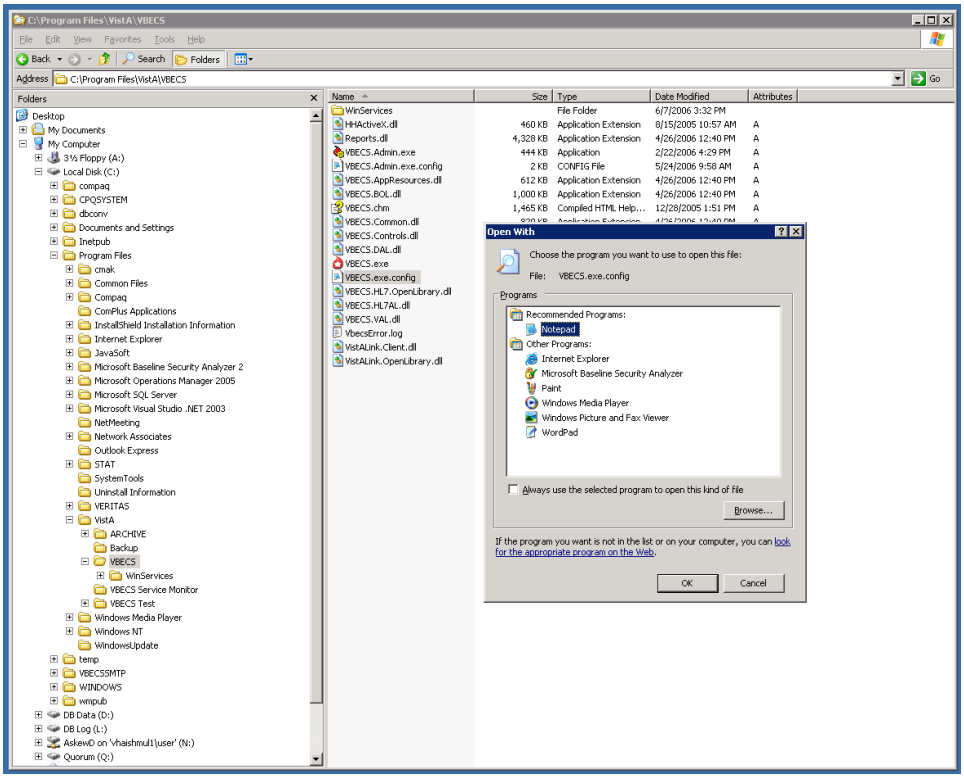
1) To update the refresh interval, locate the VBECS.exe.config file in the installation directory for VBECS: C:\Program Files\VistA\VBECS (Figure 71).

**Figure 71: Example of a Directory Structure**



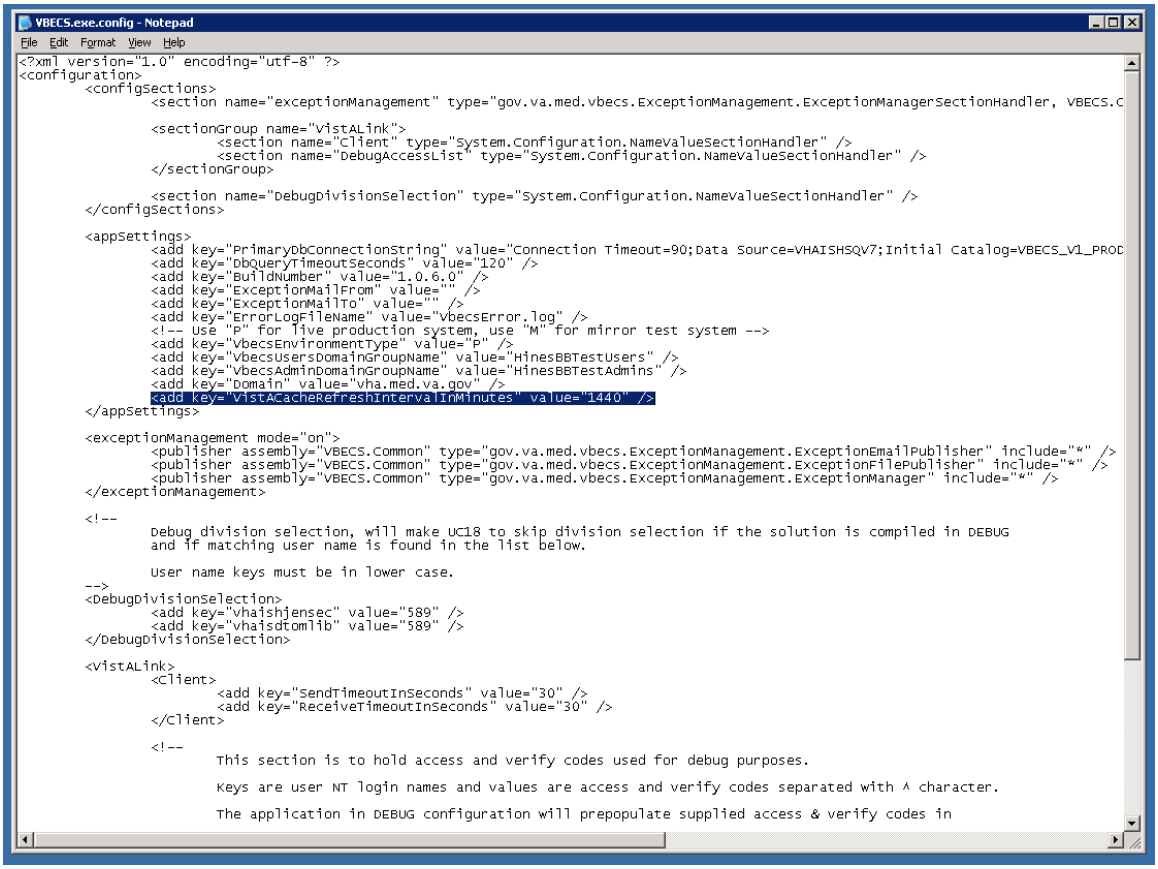
2) To open the file, right click it. Select **Notepad** (Figure 72). Click **OK**.

**Figure 72: Example of the Open With Dialog**



3) In the VBECS.exe.config file, find the entry for “VistACacheRefreshIntervalInMinutes” (Figure 73).

**Figure 73: Example of a Configuration file**




4) Edit the value to whatever is required. Save the file. This value is in minutes, so the current value of 1440 minutes is equivalent to 24 hours (to convert minutes to hours, divide by 60).

## VBECS Exception Logging

VBECS logs all errors that occur in the system in the application event viewer on the cluster. A user defined as an administrator on the cluster can connect to the cluster through Remote Desktop Connection to view these errors.

1) Click **Start**, **Control Panel, Administrative Tools**.
2) Open the Event Viewer and see the application section to view the errors that VBECS logs.
3) Double click the application icon on the right side of the screen list view.
4) In the list view on the right side of the screen, click the date column header to sort the errors by date.
5) Evaluate “Error” and warning errors and submit a Remedy ticket if the error was logged at the same time a VBECS user reported an error. Ignore informational messages. The VBECS development and maintenance team will investigate the ticket.

## VBECS Exception Workarounds

When an exception occurs in VBECS, click **Details**. Copy the details to the clipboard. Include all details of the exception in the Remedy ticket. A common exception that occurs within VBECS was traced to a Microsoft .NET 2003 problem that will not be resolved until VBECS is upgraded with the implementation of Microsoft .NET 2005. The exception shows in the details:

1) Exception Information

**********

Exception Type: System.NullReferenceException

Message: Object reference not set to an instance of an object.

TargetSite: IntPtr CallWindowProc(IntPtr, IntPtr, Int32, IntPtr, IntPtr)

HelpLink: NULL

Source: System.Windows.Forms

StackTrace Information

**********

at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr wndProc, IntPtr hWnd, Int32 msg, IntPtr wParam, IntPtr lParam)

at System.Windows.Forms.NativeWindow.DefWndProc(Message& m)

at System.Windows.Forms.Control.DefWndProc(Message& m)

at System.Windows.Forms.Control.WmUpdateUIState(Message& m)

at System.Windows.Forms.Control.WndProc(Message& m)

at System.Windows.Forms.ScrollableControl.WndProc(Message& m)

at System.Windows.Forms.ContainerControl.WndProc(Message& m)

at System.Windows.Forms.ParkingWindow.WndProc(Message& m)

at System.Windows.Forms.ControlNativeWindow.OnMessage(Message& m)

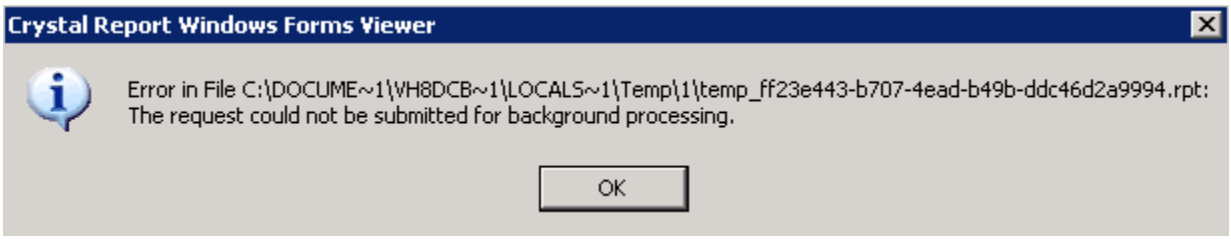
at System.Windows.Forms.ControlNativeWindow.WndProc(Message& m)

at System.Windows.Forms.NativeWindow.Callback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)

This exception occurs randomly when a screen is loading. When this occurs, the user must click **Shutdown** on the exception message and try the option again.

When the user prints a report that accepts a given date range, a Crystal Report Windows Forms Viewer window may appear (Figure 74).

**Figure 74: Crystal Reports Message**




The user may change the date range given (alter the start or end date by plus or minus one day) to resolve this problem. (This documented Crystal problem will be fixed in a future version of VBECS when Crystal Reports is upgraded.)

## VBECS Application Interfaces

**Table 7: Troubleshooting VBECS Application Interfaces**

| Source | Description of Problem | Possible Cause | Solution |
|---|---|---|---|
| VBECS: Order Alerts and Pending Order List | New orders or cancellations of existing orders in CPRS are not showing up in VBECS. | The OERR-VBECS Logical Link is not running on the VistA system. | Start the OERR-VBECS Logical Link. |
| | | The VBECS HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS HL7 Multi Listener Windows Service. |
| | | Network connectivity issue | Contact local system support. |
| VBECS Admin: Configure Division | New orders are not showing up in VBECS. | Order mappings to institutions within a division's configuration were changed. | Stop and restart the VBECS HL7 Multi Listener Service. |
| VBECS: Patient Update Alerts | VistA patient updates are not showing up in VBECS. | The patient being updated in VistA is not in the VBECS Patient table and is, therefore, not a Blood Bank patient. | No action is required. |
| | | The fields that were updated in VistA are not stored in VBECS, therefore, no data will be updated. | No action is required. |
| | | The Taskman scheduled option VAFC BATCH UPDATE is not scheduled to run or has not reached the time limit in the schedule. | Schedule the VAFC BATCH UPDATE option to run at the desired increment or use the option "One-time Option Queue" in the Taskman Management Options to start the task. |
| | | The VBECSPTU Logical Link is not running on the VistA system. | Start the VBECSPTU Logical Link. |
| | | The VBECS HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS HL7 Multi Listener Windows Service. |
| | | Network connectivity issue | Contact local system support. |

| Source | Description of Problem | Possible Cause | Solution |
|---|---|---|---|
| VBECS: Patient Merge Alerts | VistA Patient Merge events are not showing up in VBECS. | The two patient identifiers in the merge do not exist in VBECS and, therefore, cannot be merged. | No action is required. |
| | | The VBECPTM Logical Link is not running on the VistA system. | Start the VBECSPTM Logical Link. |
| | | The VBECS HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS HL7 Multi Listener Windows Service. |
| | | Network connectivity issue | Contact local system support. |
| VistA: HL7 System Link Monitor | The VistA HL7 System Link Monitor shows more MESSAGES TO SEND than MESSAGES SENT for the OERR-VBECS Logical Link and is hung in an "Open" state. | The VBECS HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS HL7 Multi Listener Windows Service. |
| | | Network connectivity issue | Contact local system support. |
| | The VistA HL7 System Link Monitor shows more MESSAGES TO SEND than MESSAGES SENT for the VBECSPTU Logical Link and is hung in an "Open" state. | The VBECS HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS HL7 Multi Listener Windows Service. |
| | | Network connectivity issue | Contact local system support. |
| | The VistA HL7 System Link Monitor shows more MESSAGES TO SEND than MESSAGES SENT for the VBECSPTM Logical Link and is hung in an "Open" state. | The VBECS HL7 Multi Listener Windows Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS HL7 Multi Listener Windows Service. |
| | | Network connectivity issue | Contact local system support. |
| CPRS: Orders Tab | CPRS does not display the correct status of a Blood Bank order after it was updated in VBECS. | The VBECS CPRS Client Monitor Windows Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS CPRS Client Monitor Windows Service. |
| | | The VBECS-OERR Logical Link is not running. | Start the VBECS-OERR Logical Link in Background mode. |
| | | Network connectivity issue | Contact local system support. |
| CPRS: Blood Bank Order Dialog | CPRS displays "Not able to open port" message in Patient Information screen in Blood Bank Order Dialog. | The VBECS VistALink XML RPC Listener Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS VistALink XML RPC Listener Service. |
| | | Network connectivity issue | Contact local system support. |
| CPRS: Reports Tab, Blood Bank Report | CPRS displays "----BLOOD BANK REPORT IS UNAVAILABLE----" | The VBECS VistALink XML RPC Listener Service is not running or is locked on the VBECS Cluster server. | Start or restart the VBECS VistALink XML RPC Listener Service. |
| | | Network connectivity issue | Contact local system support. |
| CPRS: Blood Bank Order Dialog: Signing an Order | CPRS displays an "Error Saving Order" dialog screen with the text "The error, One or more orders to the VBECS system failed and are queued for | An error occurred in the VBECS HL7 Multi Listener Windows Service, which caused a failure to respond to CPRS with acceptance. | Log onto the VBECS Cluster Server and review the System Application Event Log for error details. Click Start, Administrative Tools, Event Viewer. Select Application. |

| Source | Description of Problem | Possible Cause | Solution |
|---|---|---|---|
| | later delivery." | Network connectivity issue | Contact local system support. |
| VBECS Cluster Server Application Event Log: Source is VBECS SimpleListener | An application error has been logged to the Event Log where the Message under Exception Information is "Could not access 'CDO.Message' object." | The HL7 Multi Listener Windows Service has encountered an error trying to send an email message to the Interface Administrator | Disable port 25 blocking in McAfee. Open the VirusScan Console and select Access Protection. Click the Task menu option, the Properties. Uncheck Prevent mass mailing worms from sending mail, port 25 under Ports to block. |
| | An application warning was logged in the Event Log with the description stating, "An unsupported HL7 message was received from IP Address *[IP address]*."<br><br>The IP address in the description of the error will indicate where the message is coming from. | If the IP address is associated with the local VistA system, the HL7 Application Parameters in VistA were not set up correctly for the supported protocols. | Refer to the VBECS Application Interfacing Support Software Installation and User Configuration Guide for HL7 setup procedures in VistA. |
| | | If the IP address is not from the local VistA system, a rogue HL7 system is sending messages to the VBECS server. | Contact IRM to identify the location of the server with which the IP address is associated. Notify the site that the message is coming from the problem so that the messages can be routed to the correct location. |
| VBECS Cluster Server Application Event Log: Source is VBECS HL7 MailServer | An application error was logged in the Event Log with the source of VBECS HL7 MailServer where the Message under Exception Information is, "Could not access 'CDO.Message' object." | The HL7 Multi Listener Windows Service encountered an error trying to send an email message to the Interface Administrator. | Disable port 25 blocking in McAfee. Open the VirusScan Console and select Access Protection. Click the Task menu option, Properties. Uncheck Prevent mass mailing worms from sending mail, port 25 under Ports to block. |
| VBECS Cluster Server Application Event Log: Source is CPRS HL7 Parser | An HL7 message sent from CPRS to VBECS was rejected. The description in the Event Log is "Exception message: Division [*division]* is not supported by this instance of VBECS." | An invalid or unsupported division associated with the Patient Location was selected in CPRS when the order was created. | The order must be created in CPRS again with a valid Patient Location associated with a VBECS-supported division. |
| | An HL7 message sent from CPRS to VBECS was rejected. The description in the Event Log is "Exception message: Division [*division]* is not active in this instance of VBECS." | The division associated with the Patient Location that was selected in CPRS when the order was created is not active in VBECS. | The order must be created in CPRS again with a valid Patient Location associated with a VBECS-active division. |

## VBECS Build Version Numbers

VBECS builds are numbered as "Major.Minor.Patch.Build." "Major" is the version of the product. The "Minor" number is incremented for minor system changes. The "Patch" number is incremented for minor bug fixes. The "Build" number is incremented with each build but is not displayed publically to customers. For example, "1.2.1.0" represents the first version of VBECS with two minor system changes and one patch. VA Product Support requires the full four digits of the VBECS version number.

## VBECS Services

Problem: The VBECS Windows Services appear to be running on the cluster server and in the VistA HL7 Monitor but messages are not being sent to VistA, or messages are not being received from VistA.

Probable Cause: When the physical servers of the cluster are rebooted, or failover occurs on the cluster, or network problems cause a communication failure between VBECS and VistA it may cause the communication links to be broken and require human intervention to resolve the issue. When this happens, the services on the passive node may obtain a lock on the ports used for network communication with VistA and prevent successful message transfer.

Solution:

1. Stop the related VBECS Windows Services on both server nodes for the problem database. The services can be found in Administrative Tools (in Control Panel).
2. Start the related VBECS Windows Service on the ACTIVE node only. It is not necessary to start the passive node services.

Note: If this solution does not work, contact local IRM to restart VistA HL7 Logical Link.

Problem:
Order updates from VBECS are not being sent to CPRS to update the status of orders. The CPRS Client Monitor service appears to be running on the cluster server and the VistA HL7 System Monitor shows the VBECS-OERR Logical Link is running.

Probable Cause: Currently services are not cluster aware.

Solution:
Verify that there are pending transmission messages in the VBECS MessageLog table for VBECS Order Updates.

1. Open Enterprise Manager by clicking Start, Enterprise Manager.
2. Navigate to the VBECS database that is experiencing problems.
3. Right click on the MessageLog table and click Open Table, Return all rows. If you see entries where the MessageStatusCode is "1" and the SendingApplication is "VBECS", then there are pending order updates that need to be sent to VistA. Performing the steps in the Solution above should resolve this.

## Cluster Connectivity Lost

Problem: Connections to the cluster are lost. The cluster is not pingable by name or IP address, but individual nodes are still up.

Probable Cause: A network outage that affects both nodes simultaneously will cause the cluster to fail.

Solution:

1. Log into one of the cluster nodes and restart. Wait 1 minute.
2. Restart the other cluster node.
3. After the node in #1 has finished rebooting, verify that the cluster is back up.
4. When both nodes have restarted, stop and start services per the instructions in the previous section.

# Archiving and Recovery

The VBECS database will be backed up once daily at an established time to a tape drive. If a disaster occurs, the data in VBECS can be recovered from the backup media.

### Assumptions

- The SQL Server job that backs up the database is running correctly.
- Replacement hardware will have a tape drive that is compatible with the one lost in the disaster.

### Outcome

- VBECS data is successfully recovered.

### Limitations and Restrictions

- Only the VBECS data is backed up. The operating system is not backed up. In the event of a disaster, the operating system will have to be reinstalled and configured.

### Additional Information

- None

## *VBECS Backup*

If your servers are maintained at a data center, ignore this section since data center personnel will perform this task.

To preserve VBECS data in case of database corruption or destruction of hardware, the VBECS databases are copied over to shared storage via a scheduled job configured with the VBECS installation. VBECS is comprised of the following SQL databases: VBECS_V1_PROD and VBECS_V1_PROD_MIRROR (production) VBECS_V1_TEST and VBECS_V1_TEST_MIRROR (test VBECS account). Both production and test share the use of the msdb and master SQL databases. It is critical that every VBECS database is backed up nightly to tape. Remove the tape and take it to another location in accordance with local policy. For more technical details on backups, see *VistA Blood Establishment Computer Software (VBECS) Installation Guide*. For details on tape storage and backup frequency, refer to local policy.

## *VBECS Recovery*

*Unauthorized modifications will render this device an adulterated medical device under Section 501 of the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. Acquiring and implementing this software through the Freedom of Information Act require the implementer to assume total responsibility for the software and become a registered manufacturer of a medical device, subject to FDA regulation.*

If your servers are maintained at a data center, ignore this section since data center personnel will perform this task.

File a remedy ticket in the event of a disaster that destroys or damages the VBECS system. The VBECS team and VA Product Support will work to recover or rebuild the system.

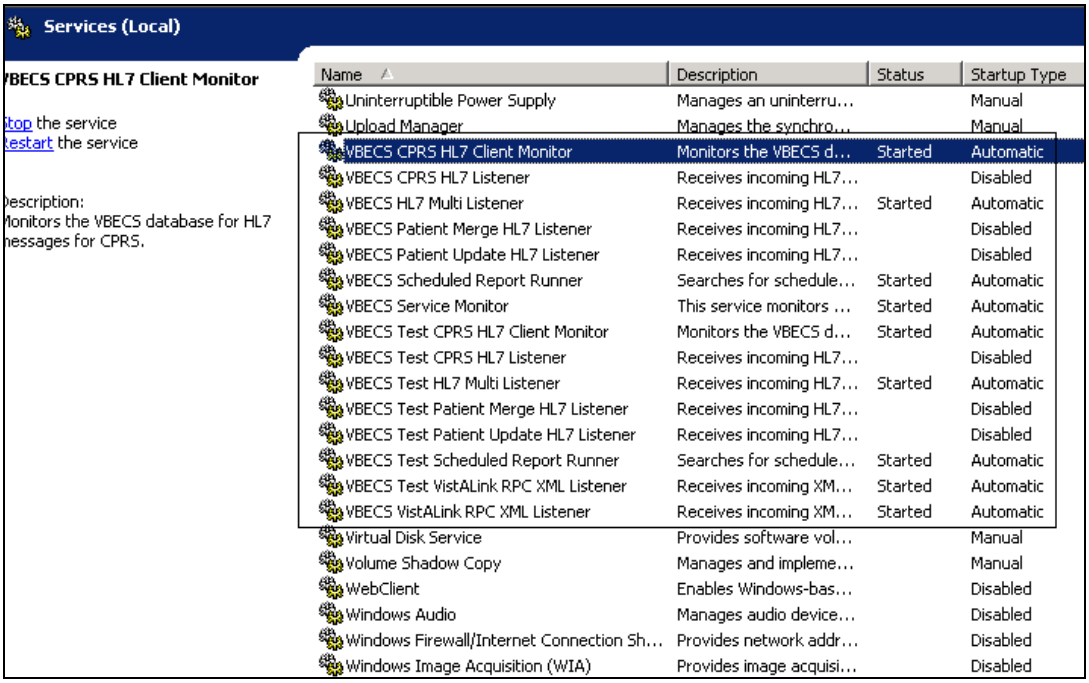
## Reinstall the System

If your servers are maintained at a data center, ignore this section since data center personnel will perform this task.

*This section should not be followed once application data has been entered. Following these steps will cause all VBECS application data to be lost.*

1) Install the image on the server hard drive.
2) Reinstall VBECS using *VistA Blood Establishment Computer Software (VBECS) Installation Guide*.
3) Make sure all VBECS Services are stopped on both servers. All VBECS service names begin with "VBECS" (Figure 75).

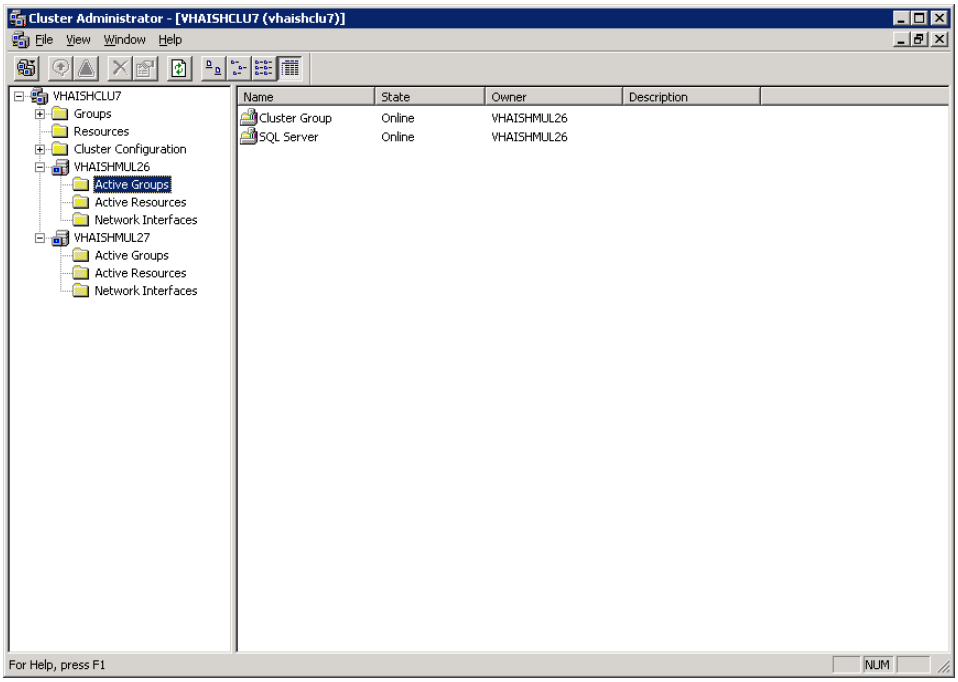
**Figure 75: Example of VBECS Services**




4) Log onto the server that is connected to the tape drive and has Backup Exec installed on it. Log in as an Administrator.

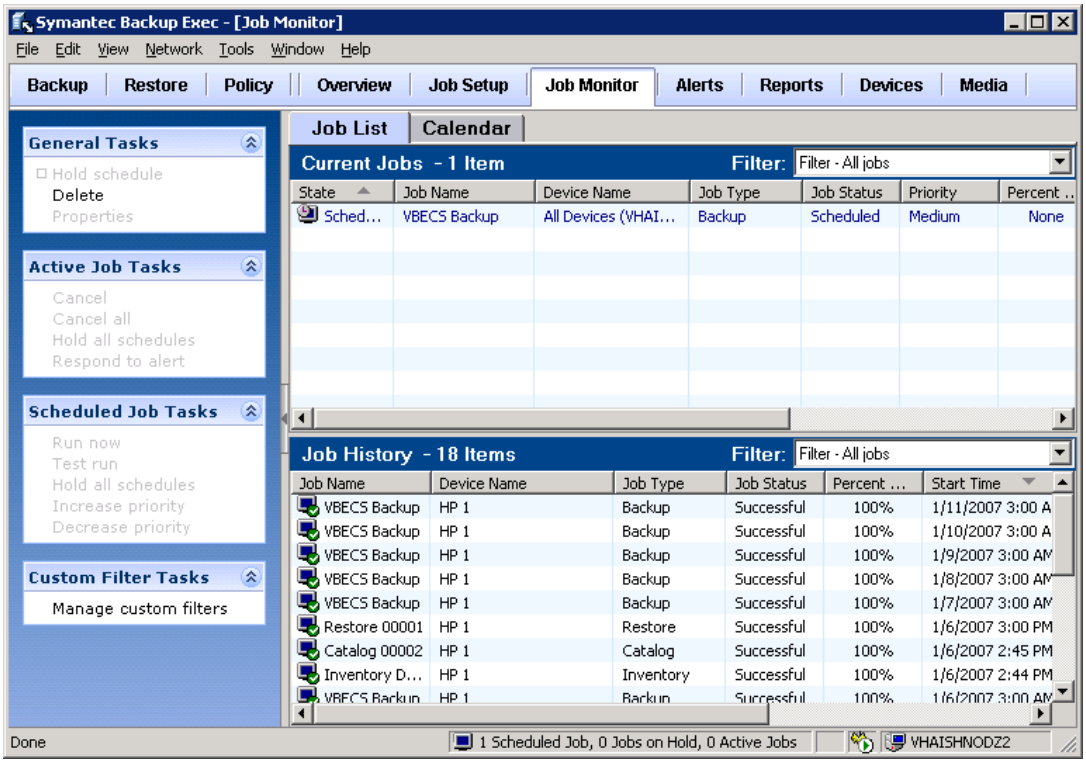
5) Open Cluster Administrator (Figure 76). Make sure this node is the active node in the cluster. If not, drag Cluster Group and SQL Server to the Active Groups folder of this node to make it the active node.

**Figure 76: Example of Cluster Administrator**



6) Click **Start**, **All Programs**, Symantec **Backup Exec 10d for Windows Servers**. The main Backup Exec console is displayed (Figure 77).

**Figure 77: Example of Backup Exec Console**

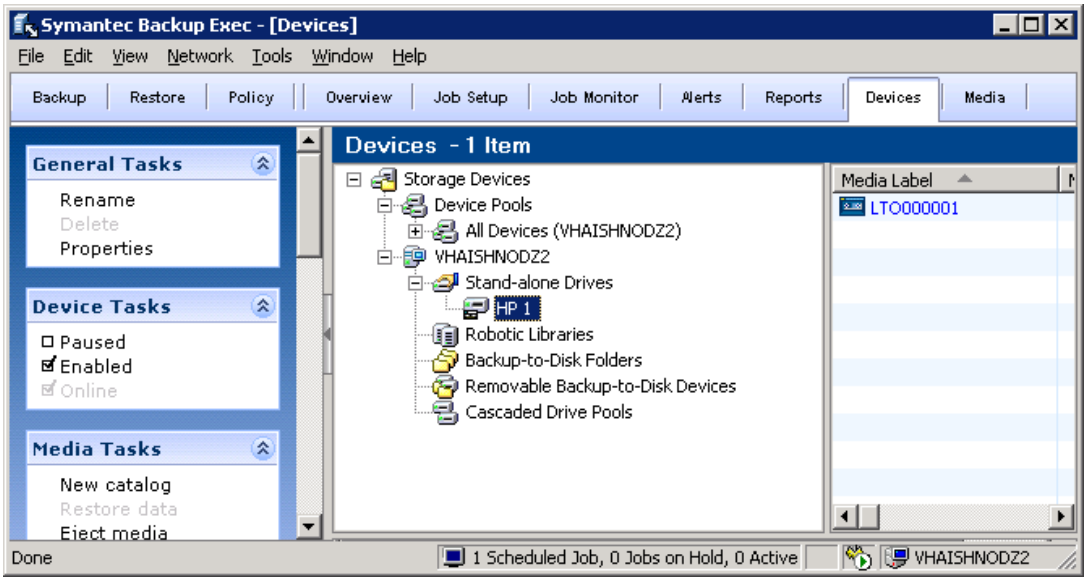



## Inventory the Tape

1) Place the tape that reflects the most recent system backup in the tape drive.
2) Click the **Devices** button (Figure 78).
3) Right click **HP 1** under the server node (not the drive pool).

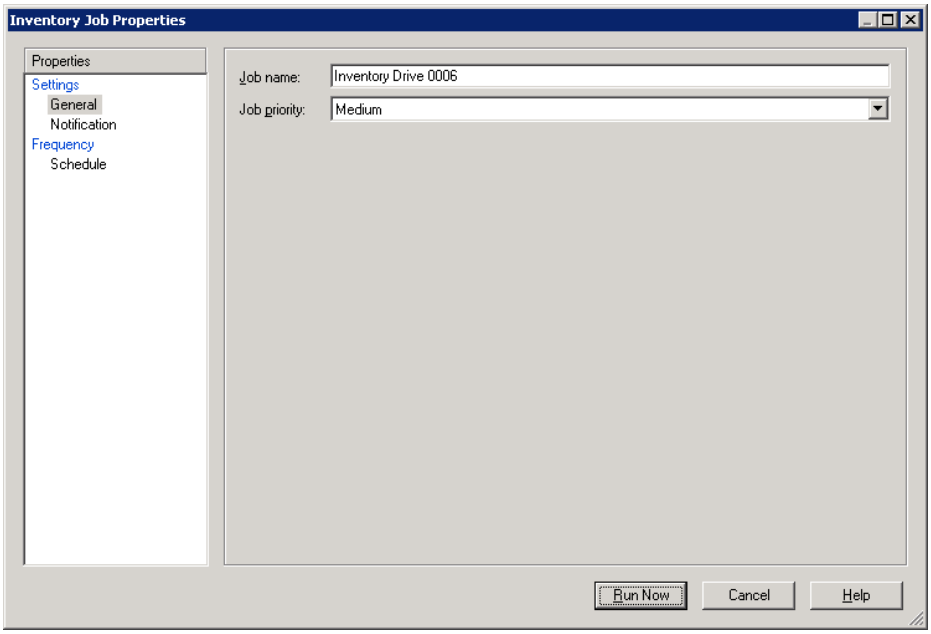
4) Select **Inventory**. The Inventory Job Properties window appears (Figure 79).

**Figure 78: Example of Devices**



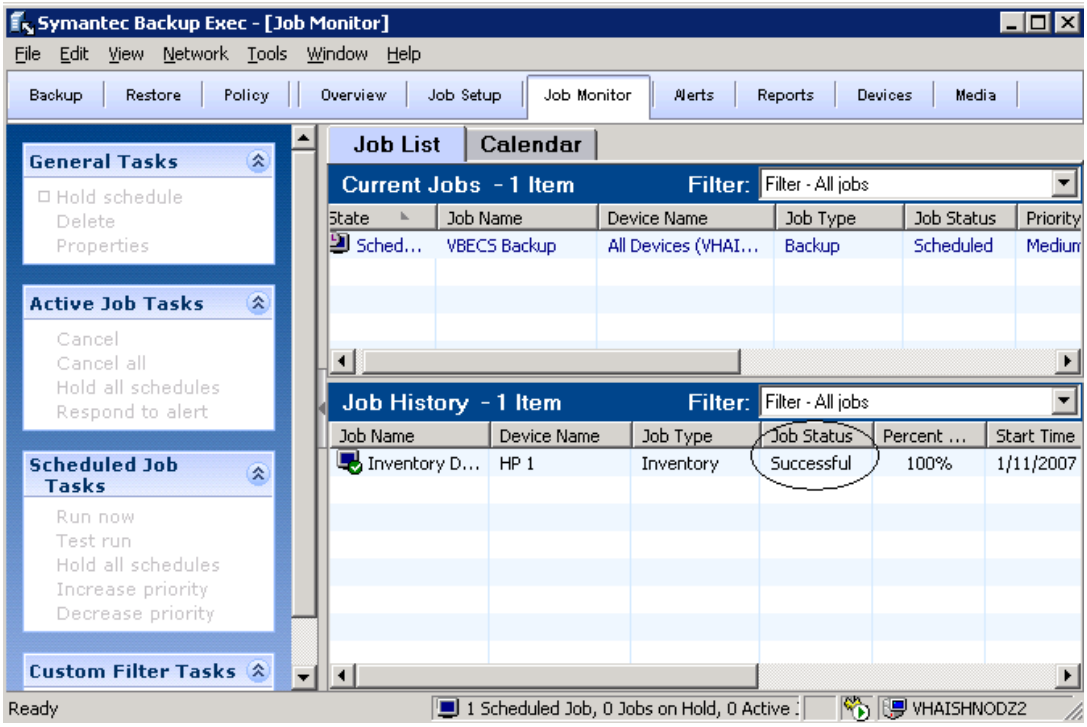

5) Click **Run Now**. Click **OK** to close information messages that appear.

**Figure 79: Example of Inventory**



6) Click **Job Monitor** (Figure 80) and make sure the job completed successfully.

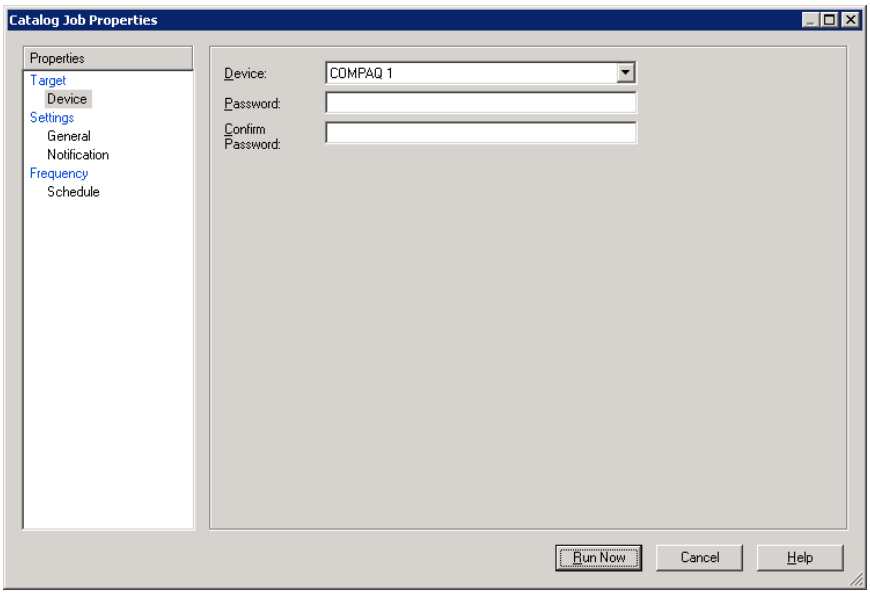
**Figure 80: Example of Successful Inventory**




## Catalog the Tape

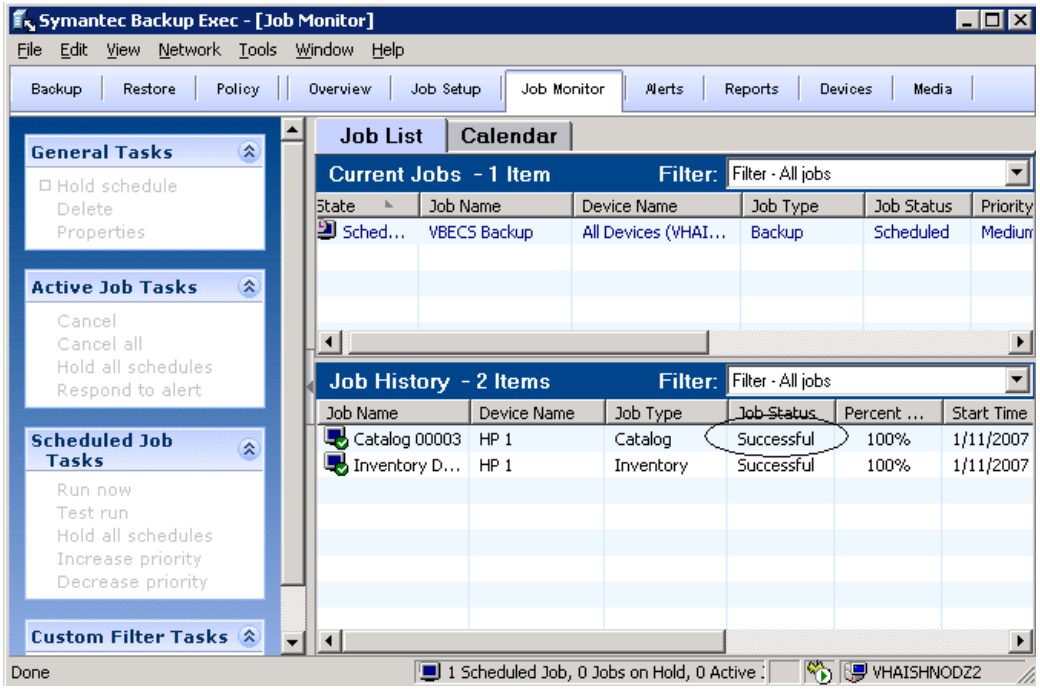
1) Click **Devices** again. Right click **HP 1** under the server node.
2) Select **Catalog**. The Catalog Job Properties window appears (Figure 81). Click **Run Now**. Click **OK** to close information messages that appear.

**Figure 81: Example of Catalog**



3) Click **Job Monitor** (Figure 82) and make sure the job completed successfully.

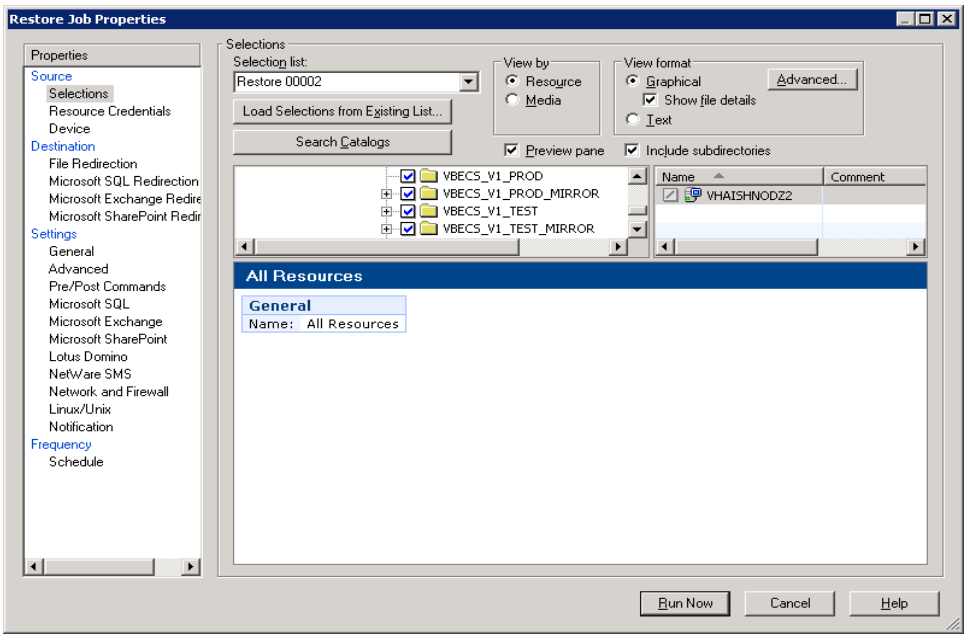
**Figure 82: Example of Successful Catalog**




## Restore Files

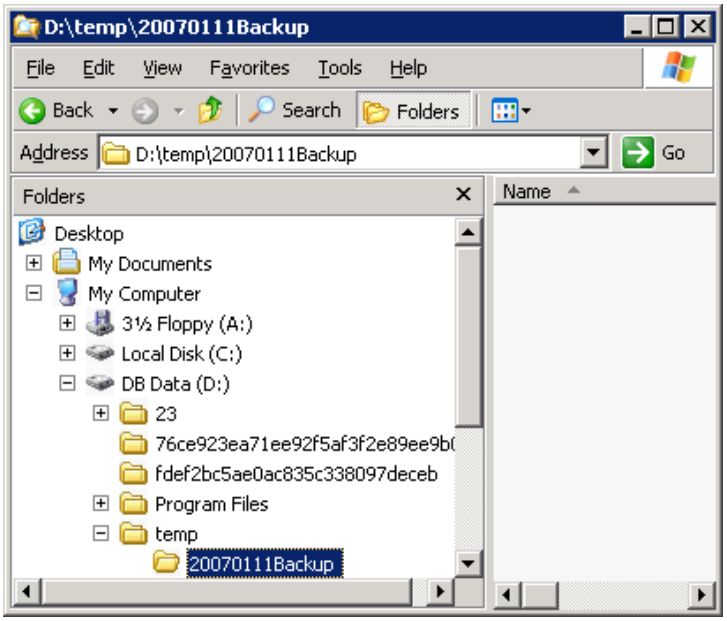
1) Click **Restore.**
2) Select all four folders under temp\Backup (Figure 83).

**Figure 83: Example of Restore Properties**



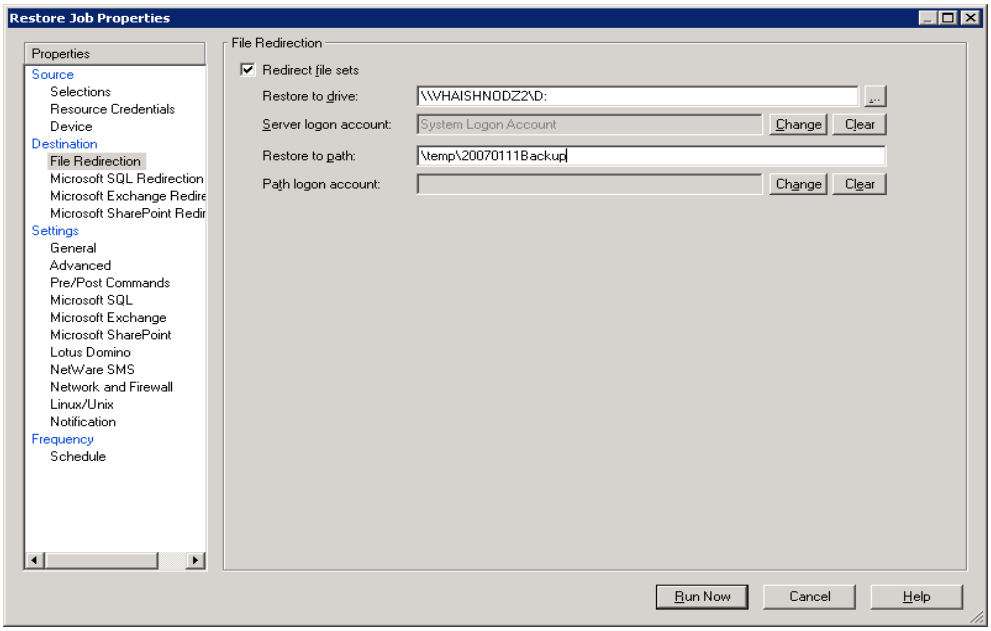
3) Create the "temp\yyyymmddBackup" directory on the D: drive (Figure 84).

**Figure 84: Example of Backup Directory**



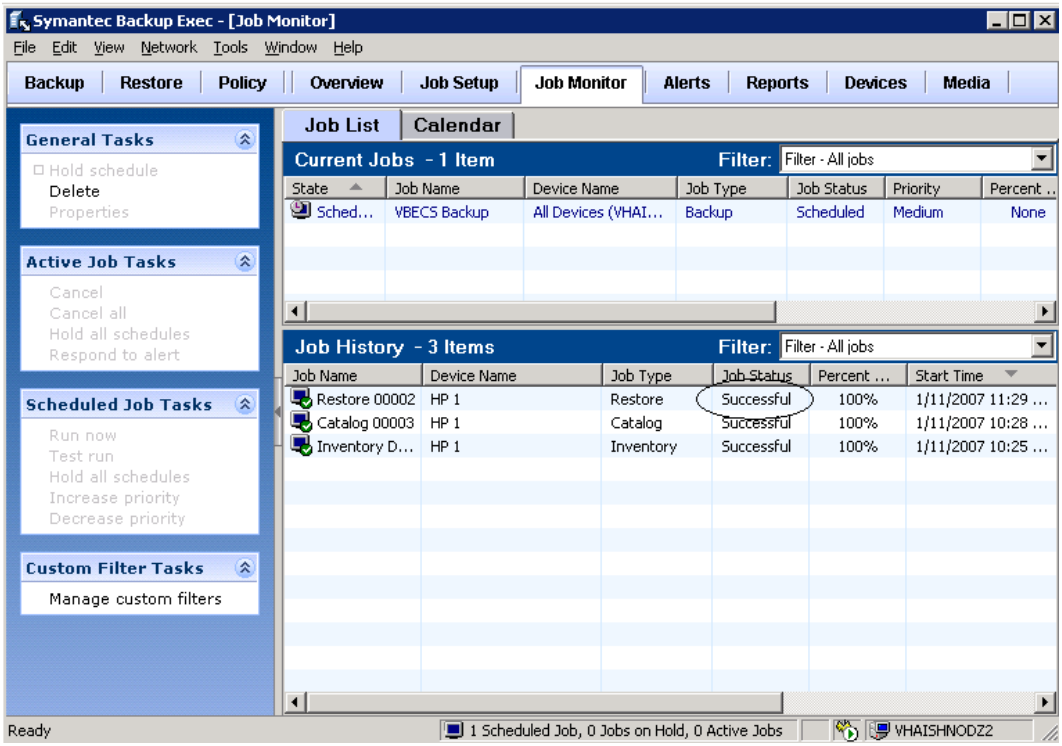

4) Click **File Redirection** on the left (Figure 85). Click the **Redirect file** sets check box.
5) In the Restore to drive field, enter **D:** (Backup Exec automatically populates the field with the server name).
6) In the Restore to path field, enter **D:\temp\yyyymmddBackup**\ (yyyymmdd represents the current date).
7) Click **Run Now**.
8) Click **OK** on information messages that appear.

**Figure 85: Example of Restore Properties**



9) Click **Job Monitor** (Figure 86) and make sure the job completed successfully.

**Figure 86: Example of Successful Restore**




## Restore the Databases

*If you find the need to perform a database restore, contact customer support to have qualified personnel assist you with the database restore.*

### VA Service Desk Primary Contact

For Information Technology (IT) support, call the VA Service Desk (VASD), 888-596-HELP (4357) toll free, 24 hours per day, 7 days per week. [Users with access to the VASD-supported request tool (e.g., Remedy) may file a ticket in lieu of calling the VASD.]

### VA Service Desk Alternate Contacts

- During business hours: As an alternate to the toll-free number, call 205-554-4710 through 205-554-4725), Monday through Friday (excluding holidays), 8:00 a.m. to 7:30 p.m. (Eastern Time).
- Outside business hours: Call 205-554-3459 through 205-554-3465, 205-554-3472, 205-554-3475, or 205-554-3482 through 205-554-3485).
- Web site: http://vaww.va.gov/emc/index.asp?s=6&p=nhd_home (VHA Enterprise Management Center)
- Email: vhacionhd@va.gov

This page intentionally left blank.

# Failover

VBECS does not have a seamless failover mechanism. If one server fails, the user will receive a message that the remote connection was lost. VBECS will lose information entered since the last save. The user must reopen a Remote Desktop Connection session. It may take 30 to 60 seconds for the Windows cluster and SQL Server running on it to fail over, which will open on the secondary server (without the user being aware of it). The user will have to reenter all information that was lost since the last save.

The connection between VBECS and VistA can be lost for a number of reasons:

- A server can fail in the VBECS cluster or the VistA server can fail. When this connection is lost, no messages can be exchanged. When the connection between VBECS and VistA is lost due to a failure of VBECS, the messages are queued on the VistA side. Orders placed during this downtime will remain in the queue. Once the VBECS system fails over and a connection is reestablished with VistA, the messages come across. The order alerts icon located in the VBECS status bar will display the orders that were in the queue at the time of failure.
- VBECS can fail because of a power outage. The UPS device will sound an alarm to alert the staff that the power is out. The IRM staff will inform the VBECS users to save their work and exit the system before the battery runs out.
- A server may fail because of a subcomponent failure such as a network interface card failure. MOM will monitor the servers for subcomponent failures. If a failure occurs, MOM will alert the IRM.

If only one node in a cluster is damaged, failover will occur. The IRM must check the MOM alerts for notification that the act occurred and fix the other node immediately to restore it to operation. When only one node is operating, no further failover can occur.

If a user's client workstation fails in the middle of a VBECS session, the session remains active on the server for a period set by the server administrator. The standard session time out is 15 minutes. If the user resolves the issues with the client workstation and reconnects to the VBECS server through Remote Desktop Connection before the session times out, the session will remain as it was when the client failed.

If a server fails due to a hardware issue, such as a network interface card failure, a Remedy ticket must be entered. If this failure occurs on only one node, users may continue to use the software after the system successfully fails over. The failover process will occur in 90 seconds. If both nodes in the cluster fail, file a Remedy ticket and refer VBECS users to Downtime Forms and Instructions in the *VistA Blood Establishment Computer Software (VBECS) User Guide*.

# Performance

VBECS may delay a critical function such as patient transfusion if the network suffers latency issues. File a Remedy ticket when latency issues arise.

VBECS was re-factored after performance testing results showed latency issues for VistA queries. As a result, many queries are cached in the VBECS database. Due to the criticality of having correct and current patient data, patient lookups cannot be cached.

## *Locking*

VBECS is designed with pessimistic locking controlled within the application code: if one user selects a record for edit, the record is locked by that user. If another user tries to edit that record, a message will tell him that the record is locked and who has the record. The second user is not granted access to the record.

Locks have a timeout period defined in the configure division portion of the VBECS Administrator application. When a lock times out or is released by a user completing his edit, another user can edit that record.

If the application code fails due to a logic bug, optimistic locking is in place to prevent data corruption. When a record is retrieved, a row version is also retrieved. When a record is saved, the row in the database gets an updated row version; before the save takes place, the save routine checks that the row version supplied matches the row version in the table. If it does not match, the routine notifies the caller that another user changed the data. The save does not complete; the user must retrieve the updated record and start his edits again.

# Security

VBECS contains sensitive data and performs a critical function, so it is critical to secure the system. It is important to secure the server from both users and malicious attacks from an individual who is trying to gain access to the system. This information section describes the measures taken to secure VBECS.

## *Active Directory*

Access to the VBECS servers is controlled through AD. Each VBECS site will have two groups set up in AD, one for normal VBECS users and one for VBECS Administrators (this is not a server administrator). Unless the user is a system administrator, he must be a member of one of these two groups to gain access to the server. Users will use their normal Windows user names to log in.

These groups also play a role in application level security. Even if a user were able to access the server, he would not be able to access VBECS.

## *Group Policy*

Group policy controls the user experience (what the user sees and has access to on the VBECS server). To configure this correctly, the recommendations in "Locking Down Windows Server 2003 Terminal Server Sessions" and "Windows Server 2003 Security Guide" (Microsoft Web site) were followed to establish a baseline for group policy.

Group policy can be applied to user accounts or to the servers directly. In the case of VBECS, group policy is applied to the servers (it is easier to manage). It is also undesirable to have group policy associated with the user, which may inhibit his use of other systems. Enabling loopback processing applies the policy to any user that logs into the server.

## *Virtual Local Area Network*

As a medical device, VBECS must exist in a segregated part of the LAN [Virtual Local Area Network (VLAN)]. The VLAN is configured to only allow necessary communication in and out of the VBECS system. Unneeded ports are blocked.

## *Microsoft Operations Manager*

Microsoft Operations Manager (MOM) is a proactive monitoring tool. MOM will constantly monitor each server for system abnormalities. If MOM detects a problem, an email will be sent to the system administrator defined during the installation process. MOM will monitor these high-level categories:

- Windows Server 2003 Operating System
- CPU health and usage
- Network interface cards
- SQL Server
- Clustering
- Memory usage
- Hard disk health and usage
- VBECS executables and services
- Windows Services

## Database Integrity

The integrity of the database is checked weekly through the CHECKDB SQL utility. This verification runs every Saturday at 12:11 A.M. through SQL Task Manager. This job generates the DatabaseIntegrityCheck.log report. The report is stored in D:\Program Files\Microsoft SQL Server\MSSQL\BACKUP\<database> folder [<database> is the VBECS environment in question (e.g., VBECS_V1_PROD, VBECS_V1_PROD_MIRROR)]. The log details the current status of tables in the database; it concludes with a message indicating the overall integrity: "CHECKDB found 0 allocation errors and 0 consistency errors in database <database>."

## Application-Wide Exceptions

Table 8 explains system exceptions to aid VA Product Support in determining the cause and resolving system issues.

**Table 8: Application-Wide Exceptions**

| System Exceptions | Description |
|---|---|
| ArgumentException | Base class for all argument exceptions. |
| ArgumentNullException | Thrown by methods that do not allow an argument to be null. |
| ArgumentOutOfRangeException | Thrown by methods that verify that arguments are in a given range. |
| ComException | Exception encapsulating COM HRESULT information. |
| Exception | Base class for all exceptions. |
| ExternalException | Base class for exceptions that occur or are targeted at environments outside the runtime. |
| IndexOutOfRangeException | Thrown by the runtime only when an array is indexed improperly. |
| InvalidOperationException | Thrown by methods when in an invalid state. |
| NullReferenceException | Thrown by the runtime only when a null object is referenced. |
| SEHException | Exception encapsulating Win32 structured exception handling information. |
| System.ArithmeticException | A base class for exceptions that occur during arithmetic operations, such as System.DivideByZeroException and System.OverflowException. |
| System.ArrayTypeMismatchException | Thrown when a store into an array fails because the actual type of the stored element is incompatible with the actual type of the array. |
| System.DivideByZeroException | Thrown when an attempt to divide an integral value by zero occurs. |
| System.IndexOutOfRangeException | Thrown when an attempt to index an array via an index that is less than zero or outside the bounds of the array. |
| System.InvalidCastException | Thrown when an explicit conversion from a base type or interface to a derived type fails at run time. |
| System.NullReferenceException | Thrown when a null reference is used in a way that causes the referenced object to be required. |
| System.OutOfMemoryException | Thrown when an attempt to allocate memory (via new) fails. |
| System.OverflowException | Thrown when an arithmetic operation in a checked context overflows. |
| System.StackOverflowException | Thrown when the execution stack is exhausted by having too many pending method calls; typically indicative of very deep or unbounded recursion. |
| System.TypeInitializationException | Thrown when a static constructor throws an exception, and no catch clauses exist to catch it. |
| SystemException | Base class for all runtime-generated errors. |

This page intentionally left blank.

# Glossary

| Acronym, Term | Definition |
|---|---|
| **ABO** | A group for classifying human blood, based on the presence or absence of specific antigens in the blood, which contains four blood types: A, B, AB, and O. The ABO group is the most critical of the human blood systems. It is used to determine general compatibility of donor units to a recipient. |
| **ABS** | Antibody screen, antibody screen test. |
| **Access Code** | A field in the VistA New Person file used to uniquely identify a user on the VistA system. |
| **Active Directory** | A hierarchical directory service built on the Internet's Domain Naming System (DNS). |
| **API** | Application Programmer Interface. |
| **CPRS** | Computerized Patient Record System. |
| **DBIA** | Database Integration Agreement. |
| **DSS** | Decision Support System. |
| **HCPCS** | Healthcare Common Procedure Coding System. |
| **HL7** | Health Level Seven. |
| **ICN** | Integration Control Number. |
| **LLP** | Lower Layer Protocol. |
| **LMIP** | Laboratory Management Index Program. |
| **MLLP** | Minimal Lower Layer Protocol. |
| **MOM** | Microsoft Operations Manager. |
| **OSI** | Open Systems Interconnect. |
| **OU** | Organizational Unit. |
| **PCE** | Patient Care Encounter. |
| **RDP** | Remote Desktop Protocol. |
| **RPC** | Remote procedure call. |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol. |
| **UPS** | Uninterruptible power source. |
| **VAISS** | VBECS Application Interfacing Support Software. |
| **VBECS** | VistA Blood Establishment Computer Software. |
| **VDL** | VistA Documentation Library. |
| **Verify Code** | A field in the VistA New Person file used to verify the identity of a user associated with an Access Code. |
| **VISN** | Veterans Integrated Service Network. |
| **VLAN** | Virtual Local Area Network. |
| **XML** | Extensible Markup Language. |

This page intentionally left blank.

# Appendices

## *Appendix A: Instructions for Capturing Screen Shots*

Throughout the technical manual-security guide, the Administrator is asked to capture screen shots to document configuration options. To capture a screen shot:

1) Open a blank document (for example, in Microsoft Word) and save it as (click **File**, **Save As**) "mmyydd Technical-Security Validation Record," or another easily identified file name.

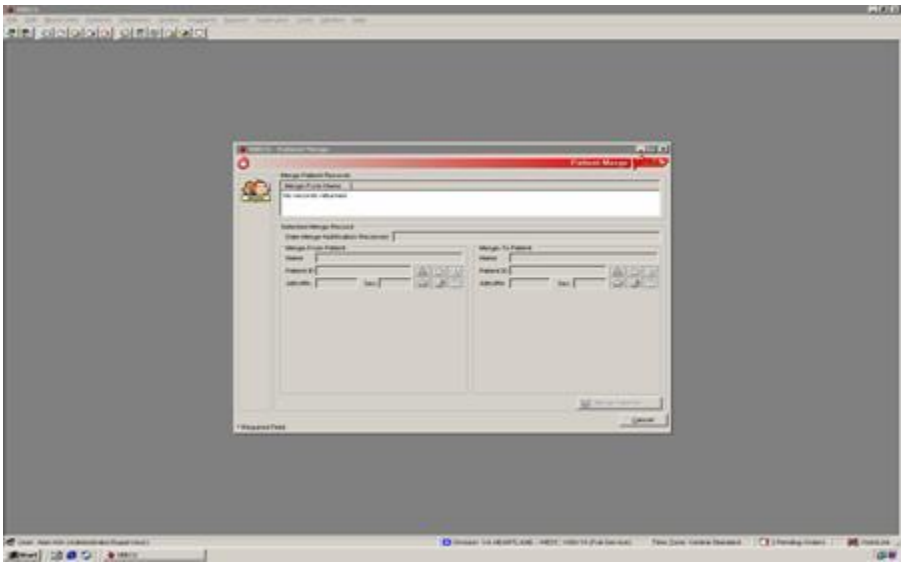
> *If you wish to place a document on both servers for ease of copying and pasting, assign file names similar to "mmyydd Technical-Security Validation Record Server1" and "mmyydd Technical-Security Validation Record Server2."*

2) When the screen you wish to capture is displayed, press the **Print Screen key**.
3) In the Technical-Security Validation Record document, place the cursor where you want to insert the picture.
4) Click  (the paste icon) or select **Edit**, **Paste (**Figure 87**)**.

**Figure 87: Paste**


5) Label the screen shot within the document with the technical manual-security guide step, page number, and server on which the picture was taken (Figure 88).

**Figure 88: Screen Shot**



This page intentionally left blank.

## *Appendix B: Workload Process Mapping to Application Option Table*

Table 9 associates record saves with workload processes. The data fields identified for transmission at the completion of a Workload Event are based on current VistA workload-related files and fields. VBECS will transmit information to a new flat file. There are no donor workload types in VBECS.

**Table 9: Workload Process Mapping to Application Option**

| Record Save Option | VBECS Process | Transaction Type [P (Patient), U (Unit), M (Miscellaneous)] | Explanation |
|---|---|---|---|
| Record a Transfusion Reaction Workup | ABO Forward and reverse typing (patient) | P | An ABO/Rh test for "pre" or "post" is enabled and a valid interpretation other than Not Tested is selected. A workload event is accrued separately for "Pre" and "Post" entries. |
| Record Patient ABO/Rh | | P | Accrue workload when a CPRS-ordered ABO/Rh test is performed. |
| Invalidate Patient Test Results* | | P | Accrue workload when a completed ABO/Rh test is invalidated. |
| Record Patient ABO/Rh | ABO Forward and reverse typing (patient) Repeat Test | M | Accrue workload when a reflex or repeat ABO/Rh test is performed, completed, and saved. |
| Invalidate Patient Test Results* | | M | Accrue workload when a reflex or repeat ABO/Rh test is invalidated. |
| ABO/Rh Confirmation | ABO forward typing (unit) | U | An ABO confirmation test is performed. When multiple units are selected in a batch, each unit in the batch accrues a workload event. Note: Workload generated during Anti-D testing is not included in the unit's confirmation test. Workload is not accrued when an ABO or Rh discrepancy override is processed and VBECS releases all patient assignments. Workload is not accrued when VBECS quarantines the unit due to a discrepancy. There is no special handling for workload collection for additional confirmation tests on a unit. |
| Edit Unit Information* | | U | Accrue workload when an ABO confirmation test is invalidated. |
| ABO/Rh Confirmation | ABO/Rh forward typing (unit) | U | An ABO/Rh confirmation test is performed. When multiple units are selected in a batch, each unit in the batch accrues a workload event. Note: Workload generated during Anti-D is part of the unit's confirmation test. Workload is not accrued when an ABO or Rh discrepancy override is processed and VBECS releases all patient assignments. Workload is not accrued when VBECS quarantines the unit due to a discrepancy. Any unit successfully confirmed accrues workload. For split modifications: workload is not inherited by split units. A split unit that requires confirmation accrues confirmation workload at the time of testing. There is no special handling for workload collection for additional confirmation tests on a unit. |
| Edit Unit Information* | | U | Accrue workload when an ABO/Rh confirmation test is invalidated. |
| Accept Order | Accept Order | M | Accrue workload when an order is accepted. When a multiple orders are selected, each order accrues workload. |

| | | | |
|---|---|---|---|
| Enter Antibody Identification Results | Antibody identification Work-Up | P | User enters additional workload associated with the individual reflex-ordered ABID. The selected VBECS multiplier will multiply against the VistA multiplier and display the (multiplication) product on the Division Workload Report. |
| Invalidate Patient Test Results* | | P | Accrue workload when the ABID is invalidated. |
| Record a Transfusion Reaction Workup | Antibody Screen (patient) | P | An ABS test for “pre” or “post” is enabled and a valid interpretation other than Not Tested is selected. A workload event is accrued separately for “Pre” and “Post” entries. |
| Record Patient Antibody Screen | | P | Accrue workload when an ordered ABS test is performed. |
| Invalidate Patient Test Results* | | P | Accrue workload when a completed ABS test is invalidated. |
| Record Patient Antibody Screen | Antibody Screen (patient) Repeat Test | M | Accrue workload when a reflex or repeat ABS test is performed, completed, and saved. |
| Invalidate Patient Test Results* | | M | Accrue workload when a reflex or repeat ABS test is invalidated. |
| Unit Antigen Typing / Patient Antigen Typing | Antigen phenotyping, Single Test phase (QC) | M | Accrue workload when Antiserum QC in Unit or Patient Antigen Typing includes the testing of both the positive and negative control cells, per specificity by lot number, when only one phase of reactivity is chosen for the test grid (IS or AHG). One workload event is collected per completed tab for regular or repeat antigen tests. |
| Unit Antigen Typing / Patient Antigen Typing | Antigen phenotyping, Multiple Test phases (QC) | M | Accrue workload when Antiserum QC in Unit or Patient Antigen Typing includes the testing of both the positive and negative control cells, per specificity by lot number, when only multiple phases of reactivity are chosen for the test grid, IS/RT, RT/37, or weak D. One workload event is collected per completed tab for regular or repeat antigen tests. When weak D is the selected test, QC may not be accrued for the rack selection. QC is accrued when positive and negative cells must be tested for the lot number. |
| Cancel Pending Order | Cancel Order | M | Accrue workload when an order on the pending order list is canceled. When multiple orders are canceled, each order accrues workload. |
| Cancel Active Order | Cancel Order | M | Accrue workload when an order on the pending task list is canceled. When multiple orders are canceled, each order accrues workload. |
| Select Units for Crossmatch | Crossmatch unit, electronic | P | This process is invoked when an individual unit is selected for patient assignment and the unit is electronically crossmatched. When multiple units are selected, each unit accrues workload. |
| Enter Crossmatch Results | Crossmatch unit, serologic immediate spin | P | Accrue workload when an individual unit crossmatch is selected to include only the IS phase, is completed, and is saved. When multiple units are selected, each unit accrues workload. |
| Invalidate Patient Test Results* | | P | Accrue workload when a completed crossmatch test is invalidated. This applies to the workload originally saved with the serologic immediate spin test. |

| | | | |
|---|---|---|---|
| Record a Transfusion Reaction Workup | Crossmatch unit, serological Coombs | P | A crossmatch test for “pre” or “post” is enabled and a valid interpretation other than Not Tested is selected. A workload event is accrued separately for “Pre” and “Post” entries.<br>When multiple units are selected, each unit accrues workload. |
| Enter Crossmatch Results | | P | Accrue workload when an individual unit crossmatch is selected to include all phases or only the AHG phase, is completed, and is saved. When multiple units are selected, each unit accrues workload. |
| Invalidate Patient Test Results* | | P | Accrue workload when a completed crossmatch test is invalidated. This applies to the workload originally saved with the test, serological Coombs. |
| Enter Crossmatch Results | Crossmatch, Repeat Test | M | Accrue workload when an individual unit crossmatch is selected to include all phases or IS or only the AHG phase, is completed, and is saved. When multiple units are selected, each unit accrues workload. |
| Invalidate Patient Test Results* | | M | Accrue workload when an individual unit crossmatch is invalidated. |
| Enter Daily QC Results | Daily Rack Quality Control (QC) | M | Accrue workload when Daily QC rack completed for one individual rack includes all rows in configured QC. When multiple racks are tested, each completed and saved tab accrues a workload event. |
| Record Patient Direct Antiglobulin Test | DAT (QC) | M | Accrue workload when Reagent QC completed in Patient DAT testing includes the testing of both the positive and negative control cells, per specificity per lot number, when only one phase of reactivity is chosen for the test grid (IS or AHG). One workload event is collected per completed tab for regular or repeat antiglobulin tests (PS, IgG, Comp). |
| Record a Transfusion Reaction Workup | Direct Antiglobulin Test (DAT) | P | A DAT test for “pre” or “post” is enabled and a valid interpretation other than Not Tested is selected. A workload event is accrued separately for “Pre” and “Post “entries. |
| Record Patient Direct Antiglobulin Test | | P | Accrue workload when a DAT is completed and saved. This count is used for all antiglobulin tests (PS, IgG, Comp) when ordered from CPRS or Reflex testing. |
| Invalidate Patient Test Results* | | P | Accrue workload when a completed DAT, PS, IgG, or Comp is invalidated. |
| Record Patient Direct Antiglobulin Test | Direct Antiglobulin Test (DAT) Repeat test | M | Accrue workload when a reflex or repeat DAT test is performed, completed, and saved. This applies to all repeat antiglobulin tests (PS, IgG, Comp). |
| Invalidate Patient Test Results* | | M | Accrue workload when a completed Repeat DAT, PS, IgG, or Comp is invalidated. |
| Modify Units | Deglycerolize unit | U | Accrue workload when an individual blood unit is processed by the Deglycerolize modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Remove Final Status* | | U | An individual blood unit’s status is invalidated when the original modification process was “Deglycerolize.” |
| Discard or Quarantine Unit | Discard unit | U | Accrue workload when an individual blood unit’s status is invalidated. When a batch of units is selected, each unit accrues workload. |

| | | | |
|---|---|---|---|
| Remove Final Status* | | U | Accrue workload when a unit is discarded for waste or credit. When a batch of units is selected, each unit accrues workload. |
| Modify Units | Freeze unit | U | Accrue workload when an individual blood unit is processed by the Freeze modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Remove Final Status* | | U | An individual blood unit's status is invalidated when the original modification process was "Freeze." |
| Modify Units | Irradiate unit | U | Accrue workload when an individual blood unit is processed by the Irradiate modification type. When a batch of units is irradiated, each unit accrues workload. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Remove Final Status* | | U | An individual blood unit's status is invalidated when the original modification process was "Irradiate." |
| Modify Units | Leukoreduce unit | U | Accrue workload when an individual blood unit is processed by the Leukoreduce modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Remove Final Status* | | U | An individual blood unit's status is invalidated when the original modification process was "Leukoreduce." |
| Split a Unit | Split unit | U | Accrue workload when a unit modification of Split and a single workload event is recorded regardless of the number of units created by the modification. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Remove Final Status* | | U | A Split Unit has its unit status invalidated. A single workload event is recorded regardless of the number of units originally created by the modification. |
| Modify Units | Rejuvenate unit | U | Accrue workload when an individual blood unit is processed by the Rejuvenate modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Remove Final Status* | | U | An individual blood unit's status is invalidated when the original modification process was "Rejuvenate. " |
| Modify Units | Thaw | U | Accrue workload when an individual blood unit is processed by the Thaw modification type. When a batch of units is thawed, each unit accrues workload. This applies to Thaw FFP and Thaw Cryo. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |

| | | | |
|---|---|---|---|
| Remove Final Status* | | U | An individual blood unit's status is invalidated when the original modification process was "Thaw." This modification type is applicable to Thaw FFP and Thaw Cryo. |
| Modify Units | Wash unit | U | Accrue workload when an individual blood unit is processed by the Wash modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Remove Final Status* | | U | An individual blood unit's status is invalidated when the original modification process was "Wash." |
| Modify Units | Volume Reduce | U | Accrue workload when an individual blood unit is processed by the Volume Reduce modification type. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Remove Final Status* | | U | An individual blood unit's status is invalidated when the original modification process was Volume Reduce. |
| Issue Blood Components | Issue unit | P | Accrue workload when a unit is issued to a patient. When a batch of units is processed, each unit invokes one workload process. |
| Justify Patient ABO/Rh Change | Justification | M | Workload is accrued when a patient's ABO or Rh typing is justified. One workload event is accrued per patient justification. |
| Login Equipment | Login Equipment | M | Accrue workload when a lot number of any type of equipment is logged into the system. When multiple lot numbers are processed in a batch, each lot number's workload is counted. |
| Login Reagent | Login Reagent | M | Accrue workload when a lot number of any type of reagent is logged into the system. When multiple lot numbers are processed in a batch, each lot number's workload is counted. |
| Login Supply | Login Supply | M | Accrue workload when a lot number of any type of supply is logged into the system. When multiple lot numbers are processed in a batch, each lot number's workload is counted. |
| Maintain Specimen | Maintain Specimen | M | Accrue workload when a specimen is maintained during order acceptance and is required for acceptance of the order. Note: This is collected in addition to the accept order workload accrued by accepting an order. Marking a specimen unacceptable does not create a negative workload event. |
| Patient antigen phenotype | Patient antigen phenotype (multiple phases) | P | Accrue workload when a patient antigen phenotype test with IS/RT or IS/37 phases is completed and saved. One workload event is collected per completed tab for repeat or regular antigen tests. |
| Invalidate Patient Test Results* | | P | Accrue workload when a patient antigen phenotype test as defined by the antiserum specificity tested with any phases is invalidated. |
| Patient antigen phenotype | Patient antigen phenotype (single phase) | P | Accrue workload when a patient antigen phenotype test with AHG or IS phase is completed and saved. One workload event is collected per completed tab for repeat or regular antigen tests. |

| | | | |
|---|---|---|---|
| Invalidate Patient Test Results* | | P | Accrue workload when a patient antigen phenotype test as defined by the antiserum specificity tested with a single phases is invalidated. |
| Pool Units | Pool unit | U | Accrue workload when a pooled unit is created and a single workload event is recorded regardless of the number of units included in the pooled unit. This applies to the Pool modification type. Add/Remove unit from a pool does not accrue any workload. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Edit Unit Information* | | U | Accrue workload when a unit is inactivated if the pooled unit was created in VBECS. |
| Remove Final Status | | N/A | No effect on workload accrual when a unit is removed from a modified status that was included in a pool. |
| Discard or Quarantine Unit | Quarantine unit | U | Accrue workload when a unit is marked for quarantine. When a batch of units is selected, each unit accrues workload. |
| Free Directed Unit For Crossover | Release directed unit | U | Accrue workload when an individual blood unit with the restriction type of “directed” is released for use as an allogeneic unit. |
| Release Unit from Patient Assignment | Release unit from patient back to inventory | U | Accrue workload when an individual unit is released from patient assignment. When multiple units are selected, each unit accrues workload. |
| Discard or Quarantine Unit | Release unit from Quarantine | U | Accrue workload when a unit is released from quarantine. When a batch of units is selected, each unit accrues workload. |
| Return Issued Unit | Return Issued unit | U | Accrue workload when a unit is returned from issue status. |
| Modify Units | Thaw/pool Cryo | U | Accrue workload when an individual unit has a modification of Thaw/Pool Cryo. A single workload event is recorded regardless of the number of units included in the pooled unit. Note: Workload is not accrued when a patient assignment is processed and VBECS releases all other patient assignments. Workload is not accrued when VBECS is required to quarantine the unit. |
| Edit Unit Information* | | U | Accrue workload when a unit is inactivated (unit record inactivated) when the pooled unit was created in VBECS. |
| Remove Final Status | | N/A | There is no effect on workload accrual when a unit is removed from a modified status that was included in a Thaw/pool Cryo pool. |
| Enter Post-Transfusion Details | Transfuse Unit | U | Accrue workload when an individual blood unit’s status is updated to “transfused.“ |
| Remove Final Status* | | U | An individual blood unit’s status is invalidated when the unit was in a status of “transfused.” |
| Record a Transfusion Reaction Workup | Transfusion Reaction Investigation | P | Accrue workload when a transfusion reaction investigation is saved. This does not include workload accrued by the optional TRW serologic testing. |
| Invalidate Patient Test Results* | | P | Accrue workload when a transfusion reaction investigation previously saved is invalidated. |

| | | | |
|---|---|---|---|
| Unit Antigen Typing | Unit Antigen phenotyping, Multiple Test phases | U | Accrue workload when a unit antigen phenotype test with IS/RT or IS/37 phases is selected and completed for an individual blood unit. There is no special handling for workload collection for additional repeat antigen typing tests on a unit. |
| Edit Unit Information* | | U | Accrue workload when a unit antigen phenotype test with Multiple Test phases is invalidated for an individual blood unit. |
| Unit Antigen Typing | Unit Antigen phenotyping, Single Test phase | U | A unit antigen phenotype test with AHG or IS phase is selected and completed for an individual blood unit. There is no special handling for workload collection for additional repeat antigen typing tests on a unit. |
| Edit Unit Information* | | U | Accrue workload when a unit antigen phenotype test with Single Test phase is invalidated for an individual blood unit. |
| Incoming Shipment | Unit login | U | An individual unit record is activated as “saved” to an incoming shipment invoice. When multiple units are entered, each unit added to the database accrues workload. |
| Edit Unit Information* | | U | Accrue workload when a unit is inactivated and logged in through incoming shipment or is a pooled unit created in VBECS. When the unit was created by split modification, no workload is invalidated in this option. |
| Outgoing Shipment | Unit logout | U | An individual unit’s status is updated to “transferred” on a confirmed outgoing shipment invoice. When multiple units are selected, each unit accrues workload. Accrue workload on confirmation of the invoice, not the addition of a unit to a temporary outgoing shipment invoice: an invoice may be confirmed only once. |
| Remove Final Status* | | U | An individual unit status is invalidated when the unit had a previous unit status of “transferred.” |
| Update Equipment Record | Update Equipment Record | M | Accrue workload when a lot number of any type of equipment is updated in the system. |
| Update Reagent Inventory | Update Reagent Inventory | M | Accrue workload when a lot number of any type of reagent is updated in the system. When multiple lot numbers are processed in a batch, each lot number’s workload is counted. |
| Update Supply Inventory | Update Supply Inventory | M | Accrue workload when a lot number of any type of supply is updated in the system. When multiple lot numbers are processed in a batch, each lot number’s workload is counted. |

*Accumulates negative workload when it is associated with inactivation of a unit or removal of a final status.

## *Appendix C: Known Defects and Anomalies*

Copies of *Known Defects and Anomalies* are available at the VDL: VistA Documentation Library (VDL), VHA OI – Health Systems Design & Development Web page.

This page intentionally left blank.

## *Appendix D: Active Directory Request Form*

Fill out this form and email or fax it to your data center contact to have users added or deleted from the VBECS Active Directory groups. Email or fax it to your data center contact for action. Contact the Implementation Team to verify your data center contact, if necessary. The data center administrator facilitating this request will return this form to you when the changes are completed.

### Blood bank information

| | |
|---|---|
| Site Name: | |
| Site identifier: | VISN number: |
| Contact name: | Phone number: |
| Email: | Fax Number: |

### Data Center information

| | |
|---|---|
| Technician name: | Phone number: |
| Email: | Fax number: |

### VBECS Users (users of normal VBECS): RnnxxxVbecsUsers group (nn is data center identifier and xxx is site identifier)

Specify the action, name and Windows ID of each technician requiring a change in access. The data center administrator will fill in his/her initials in the last column to confirm the change.

| Row | Action | Last name, first name | Windows ID | Initials (for data center administrator only) |
|---|---|---|---|---|
| 1 | Add ☐ Delete ☐ | | | |
| 2 | Add ☐ Delete ☐ | | | |
| 3 | Add ☐ Delete ☐ | | | |
| 4 | Add ☐ Delete ☐ | | | |
| 5 | Add ☐ Delete ☐ | | | |
| 6 | Add ☐ Delete ☐ | | | |
| 7 | Add ☐ Delete ☐ | | | |
| 8 | Add ☐ Delete ☐ | | | |
| 9 | Add ☐ Delete ☐ | | | |
| 10 | Add ☐ Delete ☐ | | | |
| 11 | Add ☐ Delete ☐ | | | |
| 12 | Add ☐ Delete ☐ | | | |
| 13 | Add ☐ Delete ☐ | | | |
| 14 | Add ☐ Delete ☐ | | | |
| 15 | Add ☐ Delete ☐ | | | |
| 16 | Add ☐ Delete ☐ | | | |
| 17 | Add ☐ Delete ☐ | | | |
| 18 | Add ☐ Delete ☐ | | | |
| 19 | Add ☐ Delete ☐ | | | |
| 20 | Add ☐ Delete ☐ | | | |

**VBECS Administrators (users of administrative unit of VBECS): RnnxxxVbecsAdministrators group (nn is data center identifier and xxx is site identifier)**

Specify the action, name and Windows ID of each technician requiring a change in access. The data center administrator will fill in his/her initials in the last column to confirm the change.

| Row | Action | Last name, first name | Windows ID | Initials (for data center administrator only) |
|---|---|---|---|---|
| 1 | Add ☐ Delete ☐ | | | |
| 2 | Add ☐ Delete ☐ | | | |
| 3 | Add ☐ Delete ☐ | | | |
| 4 | Add ☐ Delete ☐ | | | |
| 5 | Add ☐ Delete ☐ | | | |
| 6 | Add ☐ Delete ☐ | | | |
| 7 | Add ☐ Delete ☐ | | | |
| 8 | Add ☐ Delete ☐ | | | |
| 9 | Add ☐ Delete ☐ | | | |
| 10 | Add ☐ Delete ☐ | | | |

# *Appendix E: Data Center Instructions*

## Purpose

This appendix describes the tasks that must be completed by the data center for a successful VBECS installation, and is divided into 3 main sections depending on when the activities take place:

- Initial Setup Tasks: These tasks must be completed prior to installation of any VBECS systems.
- Ongoing Tasks: These are continual maintenance tasks.
- Installation Time Tasks: These tasks are to be completed at the time of a VBECS installation.

## Initial Setup Tasks

Execute these tasks once, prior to setting up the VBECS systems in the data center.

### Active Directory

#### VBECS User and Server Administrator Requirements

VBECS depends on Active Directory for remote server access for both VBECS and administration.

Set up two groups set up in Active Directory. The groups must have a "Universal" scope and a "Security" type.

- R*nnxxx*VbecsUsers (replace *nn* with your two-digit region number and *xxx* with the site location code): These are normal users of the VBECS system. Members of this group will have access to the server and are allowed to launch the VBECS application.
- R*nnxxx*VbecsAdministrators (replace *nn* with your two-digit region number and *xxx* with the site location code): These are users who must access the administrative component of VBECS. Members of this group will have access to the server and are allowed to launch the VBECS Administrator application.

Create a server administrator group to be shared across servers. This group must have a "Universal" scope and a "Security" type. This group will have administrative access to the VBECS servers at installation:

- R*xx*VbecsServerAdmins (replace *xx* with your two-digit region number): These are traditional server administrators who need full administrative privileges to the system. For MOM support, add the VA IT Engineering CIS Monitoring Team group to this administrator group.

#### VBECS Server Requirements

For Group Policy purposes, VBECS servers will reside in their own OU, which will contain only VBECS servers. You may also create OUs under the main OU for organizational purposes. For more information, see the Group Policy section.

### Group Policy

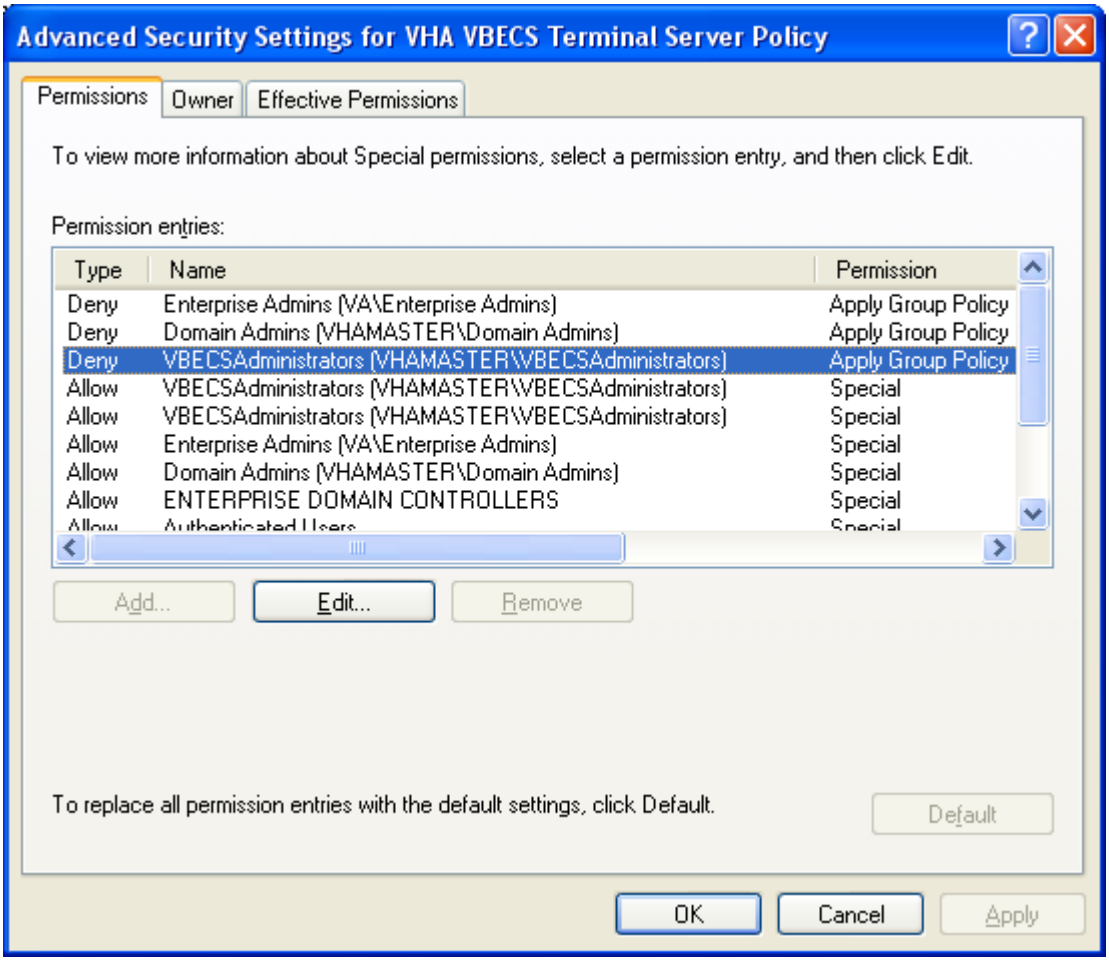
Import the VHA VBECS Terminal Server Policy from the VHAMASTER domain. If the VBECS development team changes the policy, import it again.

When importing the policy, clear the VBECS Windows Software Update Services settings (see Computer Configuration/Administrative Templates/Windows Components/Windows Update).

Place the group policy in the top-level server OU. For more information about OUs and server organization, see the Active Directory section.

Configure the policy so that it is not applied to the R*xx*VbecsServerAdmins Active Directory group. See the example in Figure 89.

**Figure 89: Example of a Group Policy Not Applied to VBECSAdministrators Group**




### Service Accounts

VBECS requires dedicated service accounts for Microsoft Cluster and Microsoft SQL Server. Add these accounts to your R*xx*VbecsServerAdmins group. Define these service accounts once to be shared across VBECS servers (*xx* represents the two-digit region number):

- Microsoft Cluster: R*xx*VBESVCCLU01
- Microsoft SQL Server: R*xx*VBESVCSQL01

At installation, give the passwords for these accounts to the installer.

### Terminal Server License Server

VBECS is a Terminal Server application and requires a license. Ensure that there is at least one Terminal Server License server set up for your domain.

### VLAN

Since VBECS is a medical device, VBECS servers and printers must reside in a VLAN. Do not turn on the VLAN until installation is complete. Since this is a data center installation, the servers will reside on a VLAN separate from that of the printers, which reside at the blood bank.

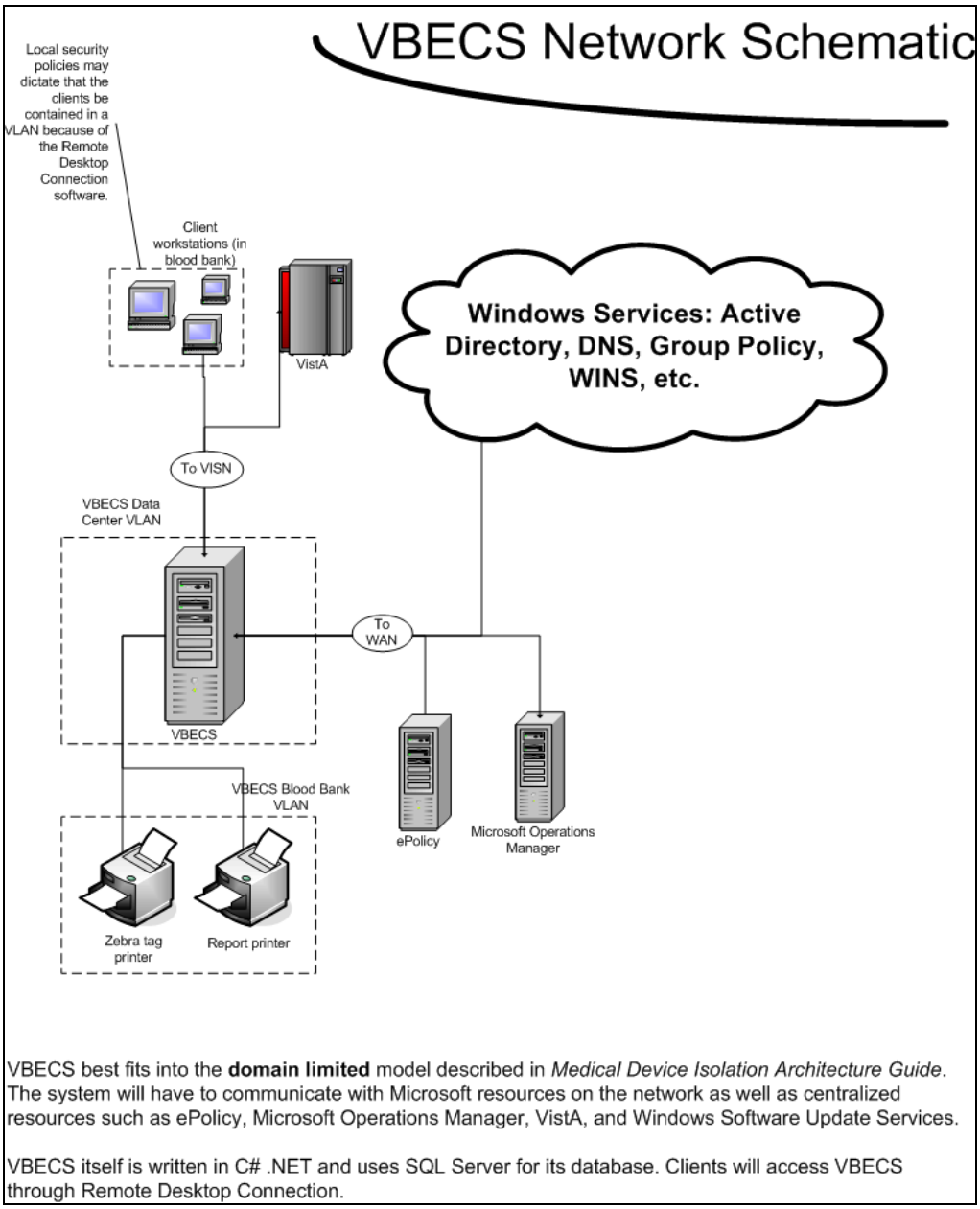
Table 10 details the communication requirements for the VLAN. Figure 90 depicts how VBECS resides in the network.

**Table 10: VBECS Communication Requirements**

| Servers, Workstations, Printers | IP Address | Notes |
|---|---|---|
| Data center domain controllers (all), WINS, DNS | See data center network administrator | |
| Data center WSUS | See data center network administrator | |
| VHAMASTER WINS | 10.3.29.33<br>10.3.29.34<br>10.39.129.200 | |
| va.gov domain controllers | 10.3.21.197<br>10.3.30.1<br>10.2.21.27<br>10.204.1.10<br>10.3.21.193 | |
| med.va.gov domain controllers | 10.2.21.26<br>10.4.229.41<br>10.3.30.2<br>10.3.21.194<br>10.30.20.27 | |
| VHAMASTER (vha.med.va.gov) domain controllers | 10.4.229.2<br>10.5.21.192<br>10.4.21.192<br>10.6.21.192<br>10.2.21.192<br>10.191.10.7<br>10.6.197.13<br>10.1.21.192<br>10.3.27.33<br>10.3.21.192<br>10.224.151.15<br>10.190.40.20<br>10.40.198.21<br>10.63.196.55<br>10.15.32.250<br>10.189.77.230<br>10.222.228.3<br>10.189.110.3<br>10.61.192.172<br>10.61.192.139<br>10.189.1.1<br>10.224.151.90<br>10.208.13.14<br>10.3.30.25<br>10.189.37.217<br>10.189.46.203 | |
| VISN WINS | See VISN network administrator | |
| VISN domain controllers | See VISN network administrator | Due to DNS “round robining,” all local domain controllers must be accessible. |

| Servers, Workstations, Printers | IP Address | Notes |
|---|---|---|
| VistA | See your network administrator | |
| MOM | 10.3.31.51<br>10.3.31.52 | |
| ePolicy | 10.204.9.190 | |
| VBECS workstations | See Appendix D: Blood Bank Configuration Checklist (installation guide) | |
| VBECS printers (label and report) | See Appendix D: Blood Bank Configuration Checklist (installation guide) | If the printers reside at the same location as the servers, just place them in the same VLAN. |

**Figure 90: VLAN Schematic**




## Ongoing Tasks

Execute the tasks in this section continually.

### Back Up the VBECS Database

Back up the VBECS database nightly:

- Back up all folders and files in the \\<cluster name>\d$\Program Files\Microsoft SQL Server\MSSQL\BACKUP directory.
- Maintain backups for at least seven days.

### VBECS Updates

When the VBECS development team releases a VBECS patch, install the patch in accordance with instructions supplied by the development team.

### Windows Updates

The VBECS development team must test every Microsoft Windows update. Once the development team is satisfied that the update causes no adverse effects, a VistA information patch in the VBEC (yes VBEC) namespace will be created by the VBECS. This patch will describe where to obtain the update and how to apply it. The patch will be released to customers by VA Product Support.

Installation of patches needs to be coordinated with the blood bank manager since most updates require a reboot.

## Installation Time Tasks

### Complete the Checklists and Password List

Complete these checklists and password list in the *VistA Blood Establishment Computer Software (VBECS) Installation Guide* prior to installation:

- Appendix B: Blood Bank Hardware Checklist: This checklist helps ensure that the correct server hardware is on-site.
- Appendix E: Server Configuration Checklist: This checklist contains server details such as names and IP addresses.
- Appendix H: Password List: This list includes passwords for the cluster and SQL server user IDs.

### Update the VBECS Server Administrators Group

Refer to the appendices in the *VistA Blood Establishment Computer Software (VBECS) Installation Guide* to complete the installation of VBECS:

- Add the installers to the VBECS Server Administrators (R*xx*VbecsServerAdmins) group. See the Windows IDs of VBECS Installers cell in the Contact Information table of the Server Configuration Checklist (Appendix E). Upon successful completion, delete the installers from the group.
- Add the executor of the VBECS data conversion to the VBECS Server Administrators group. See the Data Conversion section of the Blood Bank Configuration Checklist (Appendix D).

### Create Server Accounts

Create accounts for the VBECS servers.

# Index

## A



## B



## C



## D



## E



## F



## G



## H



## I

## K



## L



## M



## N



## O



## P



## R



## S



## T

## U



## V



## W

This is the last page of the *VistA Blood Establishment Computer Software (VBECS) 1.4.0.0 Technical Manual-Security Guide*.